

Reducción de costes en IoT

Cómo evaluar y reducir el
Coste Total de Propiedad
(TCO) en IoT

Por qué los líderes empresariales deberían dar prioridad al **Coste Total de Propiedad (TCO)** en los proyectos de IoT

El Internet de las Cosas (IoT) ha transformado las industrias al permitir operaciones más inteligentes, mejorar la experiencia del cliente y crear nuevos modelos de negocio. Sin embargo, la complejidad y la magnitud de los despliegues de IoT exigen una planificación financiera rigurosa, lo que convierte el Coste Total de Propiedad (TCO) en una métrica clave. Dar prioridad al TCO te permite evaluar el valor a largo plazo y la sostenibilidad de las iniciativas de IoT, garantizando la alineación estratégica y la eficiencia de costes.

1. Previsibilidad financiera a largo plazo

Los proyectos de IoT suelen requerir inversiones iniciales elevadas en dispositivos, infraestructura y software, además de costes operativos continuos. Centrarse en el TCO te ayuda a evitar sobrecostes, asignar los recursos de forma eficaz y reforzar la disciplina financiera.

2. Mitigación de riesgos

El análisis del TCO ayuda a identificar costes ocultos, como el mantenimiento, las actualizaciones y las medidas de ciberseguridad. Por ejemplo, los dispositivos IoT pueden ser vulnerables a ataques que generen gastos significativos derivados de brechas de seguridad.

3. Eficiencia operativa

Los sistemas de IoT integran dispositivos, redes y plataformas de datos, a menudo a lo largo de cadenas de suministro globales. El análisis del TCO pone de manifiesto áreas de optimización —como la racionalización de SKU o la gestión remota de dispositivos— que pueden reducir costes.

4. Mayor escalabilidad

Los despliegues de IoT suelen ampliarse a medida que las empresas crecen o incorporan nuevos casos de uso. Comprender el TCO garantiza que las soluciones puedan escalar sin que los costes aumenten de forma exponencial. Así, puedes valorar el equilibrio entre la inversión inicial y los beneficios a largo plazo, asegurando que las decisiones sobre

infraestructura y plataformas respalden el crecimiento manteniendo la rentabilidad.

5. Mayor confianza de las partes interesadas

Los inversores y otras partes interesadas priorizan la transparencia y la rendición de cuentas en iniciativas de gran impacto. Un marco de TCO bien definido demuestra que has evaluado en profundidad la viabilidad financiera de los proyectos de IoT, lo que refuerza la confianza y posiciona a la organización como un innovador estratégico y disciplinado.

6. Ventaja competitiva

Las empresas que controlan eficazmente los costes de IoT pueden reinvertir los ahorros en innovación, interacción con los clientes o expansión de mercado. Por ejemplo, reducir los costes del ciclo de vida de los dispositivos permite a las empresas fijar precios más competitivos u ofrecer servicios mejorados, aumentando la cuota de mercado y la fidelidad a la marca.

Conclusión

Al priorizar el TCO en los proyectos de IoT, los líderes empresariales pueden garantizar prudencia financiera, resiliencia operativa y éxito estratégico. Este enfoque integral transforma el IoT de una ambición tecnológica en un activo empresarial sostenible, permitiendo a las organizaciones prosperar en un entorno competitivo y dinámico.

Contenido

Un marco de 12 puntos para gestionar el TCO: lo conocido y lo desconocido	4
<i>Principales fuentes de coste en IoT</i>	4
<i>¿Y qué ocurre con lo desconocido?</i>	5
Panel de control de TCO: consideraciones clave de costes y cómo gestionarlas	8
Costes ocultos de recortar gastos	10
<i>Desmontando mitos – La conectividad celular es cara para IoT</i>	10
<i>Proliferación de SKU</i>	11
<i>Retiradas de dispositivos</i>	13
<i>Brechas de ciberseguridad</i>	14
<i>Interrupciones y recuperación del servicio</i>	15
Capacidades avanzadas de red, SIM y servicios que te ayudarán a reducir el TCO	16
<i>Desmontando mitos – Bajo consumo no siempre significa bajo coste</i>	18
<i>Crear un único SKU con eSIM e iSIM</i>	20
<i>Provisionamiento remoto de SIM</i>	21
<i>Gestión de dispositivos</i>	22
<i>Plataformas de habilitación de aplicaciones (AEP) con desarrollo low-code</i>	23
<i>Soluciones de extremo a extremo</i>	24
<i>Servicios totalmente gestionados</i>	25
<i>Marco de seguridad IoT</i>	26
<i>Operaciones globales 24/7</i>	27
Contacta con Wireless Logic	28

Los servicios y la conectividad IoT no son una mercancía que se pueda añadir en el último momento ni dejar en manos del usuario final para su configuración.

Integrarlos en los dispositivos y las aplicaciones desde el inicio aporta resiliencia, seguridad y la agilidad necesaria para adaptarse a condiciones de mercado cambiantes, tanto comerciales como normativas y transfronterizas.

Un marco de 12 puntos para gestionar el TCO– lo conocido y lo desconocido

El ecosistema de IoT sigue evolucionando y creciendo a gran velocidad. Como siempre, gestionar el Coste Total de Propiedad (TCO) es fundamental para el éxito a largo plazo. Sin un enfoque estructurado, los costes pueden dispararse debido a factores que a menudo se pasan por alto, como la infraestructura, el mantenimiento o los riesgos de seguridad.

Este documento presenta un marco de TCO de 12 puntos que ofrece una forma sistemática de evaluar y controlar estos costes, garantizando que los despliegues de IoT sigan siendo rentables, escalables y resilientes. Abarca las 12 áreas bien conocidas que se enumeran a continuación, pero también es esencial anticipar y abordar lo desconocido.

Principales fuentes de coste en IoT





¿Y qué ocurre con lo desconocido?

Los costes desconocidos —como los derivados de interrupciones del servicio, brechas de seguridad o el cumplimiento normativo— pueden alterar los proyectos de IoT e inflar los presupuestos. Es esencial adoptar un enfoque proactivo: una planificación sólida, la evaluación de riesgos y la implementación de dispositivos y sistemas escalables, seguros y resilientes pueden mitigar estos riesgos.

Aprovechar marcos de trabajo y socios con experiencia ayuda a anticipar retos como el cumplimiento normativo en nuevos mercados o la evolución de las amenazas cibernéticas. Aunque lo desconocido no siempre puede eliminarse, la previsión estratégica y las soluciones adaptables garantizan que puedas afrontarlo de forma eficaz, minimizando su impacto en el TCO. Estos costes desconocidos u ocultos se abordarán más adelante.



Descubre más...

...sobre cómo maximizar el tiempo de actividad y diseñar soluciones con alta disponibilidad y ciberresiliencia.

El coste de propiedad en los despliegues de IoT (Internet de las Cosas) incluye múltiples factores que comienzan con la compra inicial de los dispositivos, pero van mucho más allá.

Estos costes se generan a lo largo de todo el ciclo de vida del sistema IoT y pueden agruparse en las siguientes categorías:

Hardware

Dispositivos y sensores: Coste inicial de los dispositivos IoT, sensores y actuadores.

Gateways: Coste de los dispositivos edge o gateways para agregar y procesar datos localmente.

Sustitución y actualizaciones: Coste de la sustitución periódica o actualización de dispositivos debido al desgaste, la obsolescencia o nuevos requisitos.

Conectividad

Infraestructura de red: Implementación de redes WiFi, LoRaWAN, celulares u otros sistemas de comunicación.

Ancho de banda y planes de datos: Coste recurrente de la transmisión de datos, especialmente en despliegues IoT celulares o por satélite.

Consulta Desmontando mitos – [La conectividad celular es cara para IoT](#).

Infraestructura de red

Ten en cuenta que las redes existentes de los operadores (por ejemplo, celular o satélite) son operadas y mantenidas por los proveedores de servicio.

Evalúa los costes de planificación, instalación y puesta en marcha asociados a redes privadas (por ejemplo, WiFi o LoRaWAN).

Considera el mantenimiento a largo plazo, la seguridad y la escalabilidad de la infraestructura de red privada.

Costes de despliegue

Costes de instalación: El despliegue de dispositivos, gateways e infraestructura requiere mano de obra, herramientas y tiempo, lo que incrementa los gastos iniciales.

Complejidad de integración: Garantizar una compatibilidad fluida con los sistemas existentes aumenta el esfuerzo y los costes.

Retos geográficos: Los despliegues en ubicaciones remotas o diversas conllevan mayores costes logísticos y de recursos.

Gestión de datos

Costes de almacenamiento: El crecimiento del volumen de datos IoT exige soluciones de almacenamiento escalables y, a menudo, costosas.

Procesamiento y analítica: La obtención de información en tiempo real requiere capacidades avanzadas de procesamiento, lo que incrementa los costes operativos.

Gestión del ciclo de vida de los datos: La implementación de marcos de datos seguros (incluidas políticas de archivo, retención y eliminación) añade complejidad y costes.

El acceso y el intercambio de datos serán esenciales para muchas empresas e industrias, lo que incrementa aún más la complejidad y los costes.

Sicherheit

Inversión inicial: Minimiza los costes trabajando con socios que implementen cifrado robusto, arranque seguro y sistemas de detección de amenazas.

Mantenimiento continuo: Las actualizaciones periódicas, los parches y la monitorización para hacer frente a nuevas amenazas aumentan los costes operativos.

Mitigación de incidentes: Una respuesta inadecuada o lenta ante brechas o vulnerabilidades puede generar importantes costes de recuperación y daños reputacionales.



Software y plataformas

Suscripción a plataformas IoT: Costes de las plataformas IoT para la gestión de dispositivos, la analítica y el desarrollo de aplicaciones.

Licencias: Costes de licencias de software propietario utilizado en aplicaciones IoT.

Desarrollo a medida: Costes asociados a la creación de soluciones de software personalizadas.

Energía

Consumo energético: Costes operativos de energía de dispositivos, gateways e infraestructura de red.

Sustitución o recarga de baterías: Las decisiones de diseño y tecnología pueden ayudar a prolongar la vida útil de las baterías, aunque esto puede verse compensado por mayores costes en otras áreas.

Consulta [Desmontando mitos – Bajo consumo no siempre significa bajo coste](#).

Cumplimiento normativo

Adaptación a la normativa: Cumplir con distintos estándares normativos regionales incrementa los costes de diseño, pruebas y certificación, por ejemplo en restricciones de roaming celular o ciberseguridad.

Supervisión continua: Garantizar el cumplimiento continuo requiere monitorización, auditorías periódicas y actualizaciones, lo que aumenta los costes operativos.

Sanciones y rediseños: El incumplimiento conlleva el riesgo de multas, acciones legales y modificaciones costosas del producto.

Formación y gestión del cambio

Formación de empleados: Capacitar al personal en sistemas IoT implica costes en materiales, sesiones formativas y pérdida de productividad durante la formación.

Retos de adopción: La resistencia al cambio puede ralentizar la implantación, provocando retrasos y mayores gastos.

Soporte continuo: Las actualizaciones constantes y la necesidad de volver a formar al personal incrementan los costes operativos a largo plazo.

Experiencia del cliente (CX)

Mayores costes de soporte: Una mala experiencia del cliente genera más incidencias, aumentando los costes de soporte y mantenimiento.

Pérdida de ingresos: Una CX deficiente provoca la pérdida de clientes, elevando los costes de adquisición para sustituir a los usuarios perdidos.

Daño reputacional: Una mala CX perjudica la reputación de la marca y requiere inversiones adicionales para la recuperación y la reconstrucción de la confianza.

Escalabilidad e innovación

Ampliación de la infraestructura: Escalar requiere hardware adicional, conectividad y almacenamiento, lo que incrementa los costes.

Complejidad operativa: Gestionar despliegues de mayor tamaño aumenta los costes de mantenimiento, seguridad y cumplimiento.

Inversión en I+D: Innovar en servicios exige una inversión continua en nuevas tecnologías, actualizaciones y pruebas.

Al evaluar estos factores de forma sistemática, las organizaciones pueden identificar desde el inicio sus principales impulsores de costes y desarrollar estrategias proactivas para mitigarlos. Este enfoque integral evita gastos inesperados y alinea las decisiones tecnológicas con los objetivos empresariales.

Puede haber numerosas consideraciones adicionales, específicas del negocio o de la aplicación, además de las aquí enumeradas (por ejemplo, desmantelamiento, eliminación o reciclaje). Por ello, es importante que este marco de TCO no se utilice únicamente como una lista de comprobación, sino como un punto de partida para desarrollar una hoja de ruta hacia un éxito sostenible en IoT, ayudándote a mantener la competitividad mientras optimizas los costes en cada fase del despliegue.

Panel de TCO: *consideraciones clave de costes*

Marco de TCO de 12 puntos



Costes ocultos* de red y gastos y cómo evitarlos

Desmontando mitos

La conectividad celular es cara para

La proliferación de SKU incrementa los costes de inventario en torno a un **~20–30% anual** [NetSuite]

Una visita técnica in situ puede costar más

1.000 \$ por emplazamiento [Sightcall]

Los costes de retirada de dispositivos suelen superar los

10 M \$ [Insurance Edge]

Los ataques de ransomware a dispositivos IoT pueden superar los

5 M USD en costes [PurpleSec]

Las interrupciones no planificadas de sistemas industriales cuestan a las

empresas 100.000 \$ por hora [ABB]

* Los costes son proporcionales al tamaño de la empresa y su huella operativa.

s y cómo gestionarlas

cortar os

a IoT

s de

os

]

e

r

resa y a su

Capacidades que debes exigir a tu proveedor de servicios IoT para ayudarte a reducir el TCO



Desmontando mitos

Bajo consumo no siempre significa bajo coste



Crear un único SKU con eSIM e iSIM



Provisionamiento remoto de SIM



Gestión de dispositivos



Plataformas de habilitación de aplicaciones (AEP) con desarrollo low-code



Soluciones de extremo a extremo



Servicios totalmente gestionados



Marco de seguridad IoT



Operaciones globales 24/7



Costes ocultos de recortar gastos

Desmontando mitos – La conectividad celular es cara para IoT

Las percepciones sobre que la conectividad celular (y también la satelital) es cara para IoT han evolucionado con el tiempo, moldeadas tanto por la experiencia como por la creciente necesidad de fiabilidad y seguridad.

Con la conectividad celular, el Coste Total de Propiedad (TCO) suele ser más favorable que con WiFi, Bluetooth, LoRaWAN o Zigbee, especialmente cuando estas redes son gestionadas por terceros que no tienen participación directa en la solución IoT.

Menores costes de infraestructura

Las redes celulares son desplegadas, mantenidas y gestionadas por los Proveedores de Servicios de Comunicaciones (CSP), lo que elimina los costes de infraestructura para las empresas.

Las organizaciones simplemente pagan por los planes de datos, sin necesidad de instalar ni mantener estaciones base o conexiones de backhaul.

Las alternativas como WiFi, LoRaWAN y Zigbee requieren una inversión significativa en gateways, puntos de acceso o redes malladas, especialmente cuando no existe infraestructura pública o empresarial disponible. Cuando sí existe (como en el caso del WiFi), rara vez está optimizada para IoT, lo que provoca un rendimiento deficiente, un mayor mantenimiento y una experiencia del cliente (CX) degradada. Por ejemplo, los dispositivos IoT de terceros (no incluidos en listas aprobadas por TI o por el CISO) pueden ser bloqueados en redes corporativas o pasados por alto durante las tareas de mantenimiento.

Mantenimiento y calidad del servicio

Las redes celulares se diseñan y gestionan priorizando la fiabilidad, la resiliencia, la seguridad y la escalabilidad. No debes asumir que esto sea siempre así en las redes WiFi, por lo que es importante evaluar si existen configuraciones específicas para IoT y planes de mantenimiento adecuados. Los problemas derivados de redes sobrecargadas o mal mantenidas se traducen en mayores costes de reparación, pérdida de servicio y una CX reducida.

Riesgos de seguridad

La conectividad celular ofrece una seguridad sólida mediante autenticación basada en SIM y cifrado, minimizando las vulnerabilidades. En cambio, las redes WiFi domésticas o comerciales son más propensas a sufrir brechas de seguridad, lo que a menudo exige costosas medidas de mitigación. Una seguridad deficiente incrementa los riesgos operativos y eleva significativamente el TCO.

En resumen

El IoT celular ofrece cuatro beneficios clave y, lejos de ser costoso, suele ser la opción más inteligente y rentable para los despliegues de IoT:



Sin costes de infraestructura:
los CSP se encargan de la infraestructura

Fiabilidad:
redes gestionadas profesionalmente maximizan el tiempo de actividad

Escalabilidad:
admite despliegues a gran escala de forma fluida

Seguridad:
protocolos avanzados minimizan los riesgos

Proliferación de SKU

La proliferación de SKU —la creación de múltiples unidades de mantenimiento de stock (SKU) para cumplir requisitos regionales, funcionales o específicos de cada cliente— puede incrementar de forma significativa los costes de los despliegues de IoT.

En el IoT celular, la SIM es un factor clave que, si se pasa por alto, puede socavar otras decisiones de hardware y software tomadas en la fase de diseño del dispositivo.

Gestionar una gran diversidad de SKU genera una mayor complejidad en la producción, retos en la gestión de inventario y un aumento de los costes generales de logística y cumplimiento normativo. Esta fragmentación también complica los procesos de pruebas, certificación y soporte, incrementando el Coste Total de Propiedad (TCO) de los proyectos de IoT.

La proliferación de SKU incrementa los costes de mantenimiento de inventario en torno a un

20–30 % anual

[NetSuite]



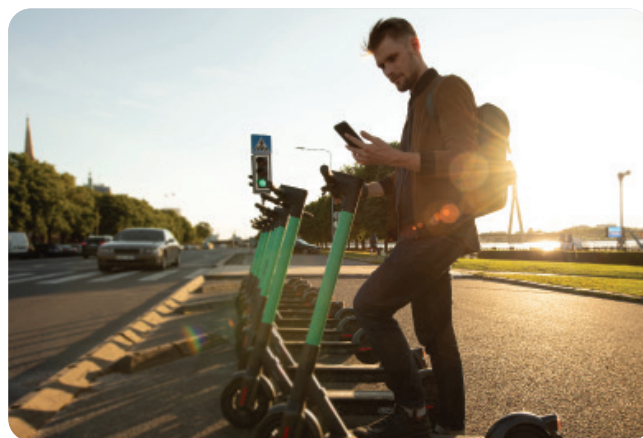
Para abordar estos retos, las empresas pueden adoptar estrategias de racionalización de SKU:

1. Diseño modular

Mediante la creación de componentes de hardware y software modulares (incluido el provisionamiento remoto de SIM), las empresas pueden ensamblar productos que satisfagan distintas necesidades sin mantener SKU independientes. Este enfoque reduce la complejidad de fabricación y mejora la escalabilidad.

2. Certificación global

Invertir en hardware y servicios de conectividad con certificación global elimina la necesidad de SKU específicos por región. Un único SKU, incluida la SIM, puede desplegarse en múltiples geografías, reduciendo los costes de cumplimiento normativo y simplificando la logística.



3. Personalización basada en software

Trasladar la funcionalidad del hardware al software permite a las empresas utilizar un único SKU de hardware con actualizaciones de software específicas por región o cliente. Este enfoque minimiza las variaciones de hardware al tiempo que maximiza la flexibilidad. Las soluciones basadas en eSIM e iSIM respaldan esta estrategia.

Al adoptar estas estrategias, las empresas pueden lograr reducciones de costes significativas, al tiempo que simplifican las operaciones, mejoran el time-to-market y mantienen la flexibilidad en los despliegues de IoT. Una racionalización eficaz de SKU es clave para optimizar el TCO en IoT y garantizar la escalabilidad a largo plazo.

En los dispositivos con conectividad celular, es fundamental analizar cuidadosamente la disponibilidad de red, especialmente en el caso de NB-IoT y LTE-M. A diferencia de LTE Cat-1, estas tecnologías no se han implementado en todos los países ni por todos los operadores a nivel global. El mismo nivel de atención es necesario en lo que respecta a la SIM. La racionalización de SKU a nivel de SIM solo es posible al trabajar con proveedores de servicios capaces de ofrecer soluciones flexibles y preparadas para el futuro (véase Crear un SKU único y seguro con eSIM e iSIM), que te permitan adaptarte a las cambiantes exigencias comerciales y normativas en distintas regiones del mundo.

Costes ocultos de recortar gastos (continuación)

Desplazamientos técnicos (Truck Roll)

Los truck rolls —el desplazamiento de técnicos de campo para instalar, mantener o reparar dispositivos IoT— son un importante factor de coste en los despliegues de IoT. Cada desplazamiento implica gastos de mano de obra, combustible, desgaste del vehículo y, a menudo, oportunidades de productividad perdidas.

Para las empresas que gestionan despliegues de IoT a gran escala o geográficamente dispersos, estos costes pueden aumentar rápidamente. Además, los retrasos derivados de la necesidad de intervención física pueden provocar interrupciones prolongadas del servicio, afectando aún más a la satisfacción del cliente y a la eficiencia operativa.

Un truck roll puede costar más de
1.000 \$ por visita
 a cada emplazamiento [Sightcall]



Para mitigar estos costes, las empresas pueden adoptar las siguientes estrategias de evitación:

1. Monitorización y gestión remotas

Aprovechar plataformas IoT que permitan diagnósticos remotos y actualizaciones de firmware reduce la necesidad de intervenciones físicas. Los dispositivos pueden supervisarse y mantenerse desde una ubicación centralizada, resolviendo muchos problemas sin necesidad de enviar un técnico.

2. Mantenimiento predictivo

La implementación de analítica basada en IA para predecir posibles fallos permite realizar intervenciones proactivas antes de que los problemas se agraven. Esto minimiza los truck rolls urgentes y no planificados, y prolonga el ciclo de vida de los dispositivos.

3. Diseño modular y acceso sencillo

Diseñar dispositivos con componentes modulares o piezas que puedan ser atendidas fácilmente simplifica el mantenimiento en campo, reduciendo la duración y la frecuencia de las visitas in situ.

Al adoptar estas estrategias, las empresas pueden reducir significativamente los costes operativos, mejorar la eficiencia del servicio y aumentar la escalabilidad de sus despliegues de IoT.

Retiradas de dispositivos

Las retiradas de dispositivos se encuentran entre los desafíos más disruptivos y costosos en los despliegues de IoT.

Una retirada puede producirse por defectos de hardware, vulnerabilidades de software, brechas de seguridad o el incumplimiento de normativas regulatorias.

Estos incidentes generan costes directos, como el envío, las reparaciones o las sustituciones, y costes indirectos como la pérdida de confianza de los clientes, responsabilidades legales y daños reputacionales. En despliegues de IoT a gran escala, las retiradas pueden escalar de forma exponencial debido al elevado volumen de dispositivos implicados y a la logística necesaria para recuperarlos o reemplazarlos.

Los costes de retirada de dispositivos suelen

superar los 10 millones de dólares

[Insurance Edge]



Para mitigar los riesgos de retirada, las empresas pueden adoptar las siguientes estrategias de prevención:

1. Pruebas rigurosas, simulación y aseguramiento de la calidad

Unos procesos exhaustivos de pruebas previas al despliegue garantizan que los dispositivos cumplan con los estándares de rendimiento y normativos. El uso de gemelos digitales para simular condiciones reales minimiza el riesgo de fallos no detectados.

2. Actualizaciones Over-the-Air (OTA)

Los dispositivos IoT equipados con capacidades de actualización OTA pueden recibir correcciones de software y parches de seguridad de forma remota, eliminando la necesidad de retiradas físicas en muchos casos.

3. Monitorización y analítica proactivas

La supervisión en tiempo real del rendimiento de los dispositivos permite identificar y resolver problemas emergentes antes de que se produzcan fallos generalizados, reduciendo el alcance de posibles retiradas.

Estas estrategias pueden implementarse mediante plataformas de gestión de dispositivos, aplicaciones y seguridad que permiten monitorizar desde la temperatura del dispositivo hasta gemelos digitales completos y los patrones de comunicación entre el dispositivo y la nube. De este modo, las empresas pueden reducir de forma significativa la probabilidad y el impacto de las retiradas, preservando la confianza de los clientes y optimizando los costes de los despliegues de IoT.

Costes ocultos de recortar gastos (continuación)

Brechas de ciberseguridad

Las brechas de ciberseguridad representan un riesgo crítico para los despliegues de IoT y, a menudo, provocan importantes daños financieros y reputacionales. Los costes directos incluyen la respuesta a incidentes, las investigaciones forenses, el tiempo de inactividad de los sistemas y las sanciones legales, mientras que los costes indirectos derivan de la pérdida de confianza de los clientes, el incumplimiento normativo y el daño reputacional a largo plazo.

En los despliegues de IoT a gran escala, la naturaleza interconectada de los dispositivos amplifica las vulnerabilidades, lo que puede permitir que una brecha comprometa redes completas o sistemas críticos.

Los ataques de ransomware a dispositivos IoT pueden superar los 5 millones de dólares en costes.

Las brechas prolongadas añaden cargas financieras significativas [PurpleSec]



Para minimizar estos riesgos, las empresas pueden adoptar las siguientes estrategias de ciberseguridad:

1. Diseño seguro de los dispositivos

Integrar la seguridad en los dispositivos IoT desde el inicio reduce la probabilidad de brechas. Esto incluye mecanismos de arranque seguro, cifrado y autenticación basada en hardware.

En los ámbitos de la banca, los pagos y la TI empresarial, métodos de autenticación como la biometría, los certificados digitales o la autenticación multifactor ya son estándar. IoT SAFE (un estándar de la GSMA) permite implementar estas estrategias de forma rentable en dispositivos IoT.

2. Actualizaciones de seguridad periódicas

La implementación de actualizaciones de firmware over-the-air (FOTA u OTA) garantiza que los dispositivos permanezcan protegidos frente a nuevas amenazas. La aplicación continua de parches ayuda a evitar la explotación de vulnerabilidades conocidas.

3. Segmentación y monitorización de la red

Aislar los dispositivos IoT de otros sistemas críticos limita la propagación de posibles brechas. La monitorización en tiempo real y la detección de amenazas refuerzan aún más la defensa.

Al integrar estas estrategias, las empresas pueden reducir de forma significativa el riesgo y el impacto de las brechas de ciberseguridad; no obstante, estos son solo tres de muchos elementos necesarios. A medida que evolucionan los métodos de ciberataque, también deben hacerlo la tecnología, las personas y los procesos dentro de tu organización. Nuestro Marco de Seguridad IoT está diseñado para ayudar a CISOs, CIOs y arquitectos de sistemas a defenderse, detectar y responder ante las amenazas de ciberseguridad en IoT.



Interrupciones del servicio y recuperación

Las interrupciones del servicio en los despliegues de IoT afectan a las operaciones, erosionan la confianza de los clientes y provocan pérdidas financieras directas.

Los costes incluyen el tiempo de inactividad, la pérdida de productividad, las penalizaciones por incumplimiento de los acuerdos de nivel de servicio (SLA) y los gastos de reparación y recuperación. Los costes indirectos, como el daño reputacional y la pérdida de clientes, incrementan aún más el impacto financiero.

El estudio Value of Reliability de ABB reveló que las interrupciones no planificadas cuestan a las empresas industriales más de 100.000 \$ por hora, y que una interrupción de ocho horas puede alcanzar el millón de dólares. Dos tercios de las empresas sufren interrupciones mensuales, y aun así el 21 % sigue utilizando un enfoque de mantenimiento reactivo (run-to-fail).

Las interrupciones no planificadas de sistemas
**industriales cuestan
a las empresas
100.000 \$ por** [ABB]



La naturaleza interconectada de los sistemas IoT puede amplificar estos riesgos, ya que los fallos en un componente pueden propagarse a través de las redes. Los costes de recuperación aumentan si las interrupciones requieren intervención manual o reparaciones in situ, especialmente en despliegues geográficamente dispersos.

Este whitepaper de Wireless Logic, [Maximising Uptime for IoT – How to achieve high availability and cyber resilience in IoT](#), ofrece orientación sobre cómo maximizar el tiempo de actividad en IoT, incluyendo métodos de alta disponibilidad para dispositivos IoT.

A continuación, se resumen tres aspectos clave:

1. Alta disponibilidad

La implementación de sistemas redundantes y mecanismos de conmutación por error garantiza la continuidad durante las interrupciones, minimizando el tiempo de inactividad. Esto se aplica por igual a los dispositivos, las redes y la infraestructura en la nube.

2. Mantenimiento predictivo

El uso de analítica para detectar y resolver problemas antes de que provoquen interrupciones evita tiempos de inactividad no planificados y reduce los costes de recuperación.

3. Monitorización proactiva y respuesta a incidentes

Los sistemas de monitorización en tiempo real, junto con respuestas automatizadas a incidentes, reducen la gravedad de las interrupciones y aceleran la recuperación.

Al adoptar estas estrategias, las empresas pueden reducir la frecuencia, la duración y el impacto financiero de las interrupciones, garantizando despliegues de IoT más resilientes y rentables.



Capacidades que debes exigir a tu proveedor de servicios IoT para ayudarte a reducir el TCO



En la primera parte de este documento, presentamos un marco de 12 puntos para identificar y gestionar los principales impulsores de costes en los proyectos de IoT.

En esta sección, resumimos algunas de las soluciones tecnológicas clave que Wireless Logic ofrece a sus clientes para ayudarles a gestionar y reducir los costes.



Desmontando mitos

Bajo consumo no siempre significa bajo coste



Plataformas de habilitación de aplicaciones (AEP)

con desarrollo low-code



Crear un único SKU con eSIM e iSIM



Soluciones de extremo a extremo



Provisionamiento remoto de SIM



Servicios totalmente gestionados



Gestión de dispositivos



Marco de seguridad IoT



Operaciones globales 24/7



Desmontando mitos: *Bajo consumo no siempre significa bajo coste*

El bajo consumo en el IoT celular no siempre implica un menor coste, principalmente porque la fragmentación de la cobertura de red y la variación en las implementaciones técnicas y comerciales de los operadores móviles (MNO) generan complejidades que, a menudo, pueden anular cualquier beneficio económico.

Estas complejidades son más acusadas en los despliegues internacionales, pero se reducen considerablemente en despliegues regionales de muy gran escala, como los proyectos de medición inteligente o las operaciones de smart cities.



¿Cuáles son estas complejidades?

1. Cobertura de red fragmentada entre regiones

NB-IoT y LTE-M no están disponibles de forma consistente en todo el mundo. Algunos MNO solo admiten una de estas tecnologías y, en ocasiones, existe una única red de cada tipo por país. Esto obliga a las empresas a integrar múltiples soluciones de conectividad. A menudo, los dispositivos necesitan compatibilidad de doble modo, lo que incrementa la complejidad del hardware y los costes. Las brechas de cobertura pueden requerir opciones de respaldo, lo que eleva los gastos operativos en despliegues de IoT globales.

2. Variabilidad en las implementaciones de los operadores

Los MNO implementan NB-IoT y LTE-M de forma diferente, con variaciones en bandas de frecuencia, protocolos de seguridad y funcionalidades de ahorro energético. Estas inconsistencias afectan a la interoperabilidad de los dispositivos, incrementan los costes de pruebas y certificación y requieren actualizaciones de firmware personalizadas. Las empresas deben invertir en optimizaciones específicas por región, lo que complica los despliegues y reduce los beneficios de coste esperados de las tecnologías de bajo consumo.

3. Roaming internacional y problemas de compatibilidad

NB-IoT y LTE-M no cuentan con acuerdos de roaming ampliamente extendidos, lo que limita su funcionamiento transfronterizo. Algunos MNO cobran por el roaming o lo bloquean por completo, obligando a contratar conectividad local. Los dispositivos pueden necesitar



soluciones multi-IMSI, eSIM o adaptaciones específicas por operador, lo que incrementa los costes. Las diferencias en certificación y regulación complican aún más los despliegues globales, haciendo que una conectividad IoT de bajo consumo y sin fricciones resulte costosa y compleja.

4. Mayores costes de certificación y cumplimiento normativo

Los dispositivos IoT deben cumplir distintos requisitos de certificación y normativas específicas de cada país debido a variaciones en las bandas de frecuencia y en las políticas de seguridad. Esto da lugar a procesos de aprobación costosos y prolongados para despliegues en múltiples regiones. Requisitos adicionales de cumplimiento, como normativas locales de seguridad, pueden incrementar aún más los costes, haciendo que las soluciones de bajo consumo resulten menos rentables a nivel internacional.

5. Complejidad en la cadena de suministro y la logística

Las variaciones regionales de NB-IoT y LTE-M obligan a las empresas a mantener diferentes SKU de dispositivos, lo que complica la fabricación, la adquisición y la distribución. Aunque un único SIM es viable mediante multi-IMSI y eSIM, la gestión de múltiples variantes de módem incrementa los costes logísticos y los riesgos de inventario. Las empresas que despliegan IoT a nivel global deben enfrentarse a cadenas de suministro fragmentadas, reduciendo las ventajas de coste normalmente asociadas a los dispositivos IoT de bajo consumo.

6. Retos del ciclo de vida del dispositivo y del future-proofing

Las tecnologías NB-IoT y LTE-M siguen evolucionando, y algunos MNO pueden retirar o modificar sus implementaciones. Las empresas corren el riesgo de desplegar dispositivos en redes que podrían dejar de existir, lo que obligaría a realizar actualizaciones costosas. Asegurar el futuro de los despliegues IoT requiere una planificación cuidadosa, que a menudo anula

los ahorros a largo plazo esperados de las tecnologías celulares de bajo consumo.

LTE Cat-1 BIS ofrece una solución más universal y rentable para despliegues empresariales multinacionales

Aunque una planificación cuidadosa y el asesoramiento adecuado pueden resolver algunas de las complejidades descritas anteriormente, existen soluciones más sencillas que solo requieren compromisos mínimos en el coste del hardware y la duración de la batería.*

LTE Cat-1 BIS aborda estos retos al ofrecer disponibilidad global (3, 4 o 5 redes por país) sobre redes 4G LTE existentes, eliminando las brechas de cobertura y las restricciones de roaming de NB-IoT y LTE-M. Admite un diseño de radio única, incluida la SIM, lo que reduce los costes de hardware y simplifica la cadena de suministro. Gracias a implementaciones estandarizadas entre MNO, minimiza las complejidades de certificación y garantiza despliegues de IoT fluidos y rentables en todo el mundo.

* Dependiente de la implementación.

Recomendamos realizar pruebas que tengan en cuenta:

- (i) la frecuencia de comunicación,
- (ii) el volumen de datos,
- (iii) el impacto de velocidades más bajas frente a más altas (kbps).



Descubre más sobre las tecnologías celulares de bajo consumo[†] y por qué deberías asociarte con Wireless Logic.

[†] Incluye NB-IoT, LTE-M y LTE Cat-1 BIS



Crea un único SKU con eSIM e iSIM

Wireless Logic lleva más de 10 años desplegando soluciones eSIM y cuenta con una amplia experiencia y sólidas alianzas con operadores móviles (MNO).

Las ventajas en seguridad física y fiabilidad de las eSIM integradas y las iSIM incorporadas ofrecen una ventaja significativa frente a las SIM extraíbles. Para maximizar estos beneficios, los OEM, proveedores de soluciones y empresas también deben aprovechar el provisionamiento remoto de SIM (RSP) para gestionar todo el ciclo de vida de la SIM, desde la fábrica hasta el campo.

Solución estándar

Nuestra solución SIM estándar es un perfil SIM multi-IMSI desplegado en una eSIM, que ofrece la máxima flexibilidad y cobertura. Multi-IMSI y eSIM permiten realizar actualizaciones y localizaciones mediante actualizaciones over-the-air (OTA). Este enfoque es fundamental para la racionalización de SKU en despliegues de IoT multinacionales.

Opciones de personalización y funcionalidad avanzada

La capacidad de descargar y cambiar IMSI y perfiles SIM de forma OTA proporciona flexibilidad y opciones de personalización que pueden diseñarse en función de tus necesidades de negocio y de despliegue. Wireless Logic dispone del ecosistema de operadores más amplio y del portafolio más completo de socios de perfiles IMSI y eSIM.

Principales beneficios para ti

Un único SKU con eSIM/iSIM y RSP garantiza una conectividad global fluida, reduciendo la necesidad de múltiples variantes de dispositivos. Las actualizaciones OTA resuelven problemas de cobertura, rendimiento o cumplimiento normativo, incluidas las restricciones de roaming permanente. Este enfoque simplifica la logística, mejora la resiliencia y garantiza la eficiencia operativa a largo plazo en despliegues internacionales de IoT.

Facilidad y coste de adopción

Wireless Logic es compatible con multi-IMSI y con todos los estándares RSP (SGP.02, SGP.22, SGP.32), lo que permite un enfoque optimizado de SKU único. Esto elimina las complejidades regionales de las SIM y reduce los costes logísticos y operativos.



Descubre más sobre multi-IMSI, eSIM e iSIM
y por qué deberías asociarte con Wireless Logic.



Provisionamiento remoto de SIM

Para obtener todo el valor de las tecnologías eSIM e iSIM, es fundamental elegir un socio de provisionamiento remoto de SIM (RSP) que cuente con la infraestructura y las relaciones con operadores necesarias.

Solución estándar

Colaboramos con proveedores líderes de RSP y SIM para ofrecer un conjunto completo de capacidades de RSP y OTA, que pueden utilizarse tanto para campañas OTA a escala de flota como para actualizar SIM individuales o grupos de SIM. Esto incluye la actualización de applets en la SIM, IMSI y perfiles eSIM.

Opciones de personalización y funcionalidad avanzada

Las campañas OTA se automatizan mediante mecanismos de polling, push y pull, con registros de auditoría y estrategias de reintento que garantizan la fiabilidad, minimizan los fallos y optimizan la conectividad IoT global sin necesidad de intervención manual.

Principales beneficios para ti

El RSP ayuda a las empresas a asegurar el futuro de su conectividad IoT y a mantener altos niveles de cobertura y resiliencia a lo largo del tiempo. Los cambios a nivel de red o de SIM realizados over-the-air permiten resolver problemas de rendimiento, comerciales o de calidad cuando surgen. El aumento de las restricciones gubernamentales u operativas sobre el roaming permanente hace que el RSP sea esencial para las empresas con despliegues internacionales.

Facilidad y coste de adopción

Wireless Logic es compatible con multi-IMSI y con los tres estándares de RSP (SGP.02, SGP.22 y SGP.32). Trabajaremos contigo para identificar y automatizar una solución que se adapte a tus procesos de negocio y a tus necesidades de despliegue. Navegar por el ecosistema RSP por tu cuenta puede ser complejo y costoso, por lo que es importante elegir y colaborar con un socio especializado como Wireless Logic.



Descubre más sobre el provisionamiento remoto de SIM
y por qué deberías asociarte con Wireless Logic.



Gestión de dispositivos

La monitorización y gestión de los dispositivos IoT a nivel de conectividad, dispositivo, seguridad y aplicación es esencial para la detección y resolución remotas de incidentes operativos y de seguridad.

Gestionar estos eventos de forma remota es clave para reducir los truck rolls y mantener el tiempo de inactividad al mínimo.

Solución estándar

SIMPro es nuestra plataforma de gestión de conectividad de quinta generación, que ha evolucionado para incluir la gestión de dispositivos (DevicePro), la seguridad (NetPro) y la gestión a nivel de aplicación (Kheiron).

Las primeras líneas de defensa son la gestión de conectividad y de dispositivos, que permiten a los responsables de IoT supervisar la ubicación, la frecuencia y el consumo de datos, así como alertar, limitar, bloquear o poner en cuarentena conexiones que incumplan los parámetros definidos.

Opciones de personalización y funcionalidad avanzada

La gestión de dispositivos te permite supervisar el estado del dispositivo (intensidad de la señal, niveles de batería, temperatura) y realizar configuraciones OTA o actualizaciones de firmware correctivas. Kheiron es nuestra plataforma de habilitación de aplicaciones, que incluye gemelos digitales y la contextualización y visualización de datos de aplicaciones.

Principales beneficios para ti

La gestión de dispositivos y los gemelos digitales minimizan los truck rolls y el tiempo de inactividad al permitir la monitorización remota, el diagnóstico y el mantenimiento predictivo. Los gemelos digitales simulan condiciones reales e identifican posibles fallos antes de que se produzcan. Combinados con actualizaciones OTA y la resolución automatizada de incidencias, permiten reducir las intervenciones manuales y garantizar un rendimiento óptimo y una alta disponibilidad de los dispositivos IoT.

Facilidad y coste de adopción

La gestión de dispositivos es obligatoria para una administración eficaz de la seguridad de los dispositivos. En sectores sujetos a legislación, como el Reglamento Europeo de Ciberresiliencia (EU Cyber Resilience Act), no debe pasarse por alto el coste del incumplimiento. En el caso de dispositivos que se comunican mediante protocolos de red estándar como HTTPS, SNMP o LwM2M, el coste de adopción e integración en los procesos de negocio es relativamente bajo.



Descubre más sobre la gestión IoT y por qué deberías asociarte con Wireless Logic.



Plataformas de habilitación de aplicaciones (AEP) con desarrollo low-code

Históricamente, las ambiciones de IoT de muchas empresas se han visto frenadas por los elevados costes de los recursos de desarrollo de software o por la frustración ante retornos de la inversión lentos o inciertos.

Las plataformas de habilitación de aplicaciones con herramientas no-code o low-code reducen la necesidad de grandes equipos de desarrolladores y/o aumentan significativamente su productividad.

Solución estándar

Kheiron es una plataforma no/low-code que simplifica el desarrollo de aplicaciones IoT mediante herramientas de arrastrar y soltar, integraciones preconfiguradas y automatización. Permite un despliegue rápido, reduciendo el tiempo y los costes de desarrollo, al tiempo que garantiza una conectividad y gestión de dispositivos fluidas.

Opciones de personalización y funcionalidad avanzada

Para necesidades más avanzadas, Kheiron ofrece gemelos digitales personalizados, creación de paneles de control e integración de gemelos digitales con sistemas empresariales. Para usuarios externos y clientes finales, los paneles pueden desplegarse en iOS, Android y navegadores web. La plataforma también puede ofrecerse como solución white label.

Principales beneficios para ti

Kheiron reduce costes, acelera el time-to-market y permite a los usuarios de negocio crear soluciones sin necesidad de profundos conocimientos de programación, mejorando la agilidad y la escalabilidad para una innovación más rápida. Además, acelera el retorno de la inversión (RoI).

Facilidad y coste de adopción

Es sencillo empezar y escalar con Kheiron mediante un modelo SaaS, o ejecutarlo on-premise si así lo prefieres.



Descubre más sobre Kheiron y por qué deberías asociarte con Wireless Logic.



Soluciones de extremo a extremo

Las empresas demandan cada vez más soluciones IoT de extremo a extremo para reducir la complejidad, acelerar los despliegues y disminuir los costes.

Otras empresas que sí cuentan con recursos internos de software e integración de sistemas buscan soluciones componibles, con sensores, hardware y conectividad inalámbrica ya integrados.

Los beneficios en coste y time-to-market provienen de minimizar la sobrecarga técnica, especialmente en áreas donde no existen capacidades internas, ya sea en sensores, hardware, conectividad o software.

Solución estándar

Nuestra plataforma de habilitación de aplicaciones IoT, Kheiron, reduce los costes de desarrollo y acelera el retorno de la inversión (RoI) de múltiples formas. Esto abarca desde el asesoramiento en la elección de sensores y conectividad, hasta el suministro, la integración y la gestión del hardware, así como soluciones preprobadas y preintegradas que pueden utilizarse para iniciar despliegues o escalar a nivel empresarial.

Opciones de personalización y funcionalidad avanzada

Atendemos tanto a clientes que necesitan soluciones de extremo a extremo fáciles de adoptar y rentables, como a aquellos que prefieren soluciones componibles, que actúan como bloques de construcción que pueden configurarse según sus necesidades y consumirse bajo un modelo OPEX si se desea. La personalización puede realizarse sobre la aplicación, el gemelo digital y los paneles de control predefinidos.

Principales beneficios para ti

Tanto si se trata de soluciones completas de extremo a extremo como de soluciones componibles, se elimina la necesidad de que las empresas obtengan, integren y gestionen hardware, conectividad y software de múltiples proveedores. Esto compensa posibles carencias de conocimiento o recursos y reduce el riesgo. Además, las empresas pueden probar y evaluar el ROI antes de comprometerse con un despliegue a gran escala.

Facilidad y coste de adopción

Los clientes pueden contratar nuestros servicios en modalidad de servicios profesionales o consumir Kheiron y las soluciones preconfiguradas bajo un modelo SaaS u OPEX.



Descubre más sobre Kheiron y por qué deberías asociarte con Wireless Logic.



Servicios totalmente gestionados

Los avances en el rendimiento de la banda ancha 4G, 5G y satelital están impulsando a las grandes empresas a adoptar cada vez más servicios de Acceso Inalámbrico Fijo (FWA) totalmente gestionados, tanto para conectividad principal como de respaldo (failover).

Las altas velocidades de 4G/5G también ofrecen una base fiable para despliegues SD-WAN, especialmente en zonas remotas donde no hay disponibilidad de fibra.

Gestionar internamente redes diversas, operadores locales y el cumplimiento normativo resulta complejo y consume muchos recursos, lo que hace imprescindible contar con una solución única y unificada para garantizar la eficiencia operativa y una conectividad global sin fricciones.

Solución estándar

Nuestros servicios basados en 4G, 5G y Starlink están diseñados para ofrecer una experiencia técnica y comercial sin complicaciones. Incluyen opciones exclusivamente celulares (4G, 5G) y opciones híbridas (Starlink, 4G, 5G) en más de 80 países a nivel global.

Opciones de personalización y funcionalidad avanzada

La solución y el servicio base están diseñados para ser universales y plug and play, con soluciones personalizadas disponibles cuando se requieren. Ofrecemos un servicio totalmente gestionado que incluye hardware (routers, antenas y cableado), instalación, gestión y optimización de dispositivos, así como sustitución in situ cuando sea necesario.

Principales beneficios para ti

Nuestro servicio FWA totalmente gestionado garantiza una conectividad fiable, escalable y rentable mediante soluciones estandarizadas, monitorización proactiva y conmutación automática por error, proporcionando una experiencia consistente en sucursales de todo el mundo, independientemente de las diferencias entre operadores o de los retos de infraestructura.

Facilidad y coste de adopción

Simplificamos la conectividad global con un único contrato para satélite y celular, una instalación rápida en 10 días, gestión remota proactiva y soporte fiable in situ. Las empresas se benefician de una adquisición simplificada, tiempo de actividad garantizado y una integración de red sin complicaciones.



Descubre más sobre la conectividad empresarial
por qué deberías asociarte con Wireless Logic.



Marco de seguridad IoT

A medida que los despliegues de IoT escalan a nivel global, los riesgos de seguridad —desde vulnerabilidades en los dispositivos hasta la interceptación de datos— se vuelven más complejos. Por ello, las empresas están dando prioridad a marcos de seguridad de extremo a extremo que protejan todas las capas de la conectividad, desde la SIM hasta la nube.

El Marco de Seguridad IoT de Wireless Logic ofrece un enfoque unificado e integrado para proteger datos y dispositivos tanto en redes privadas como públicas, ayudando a las organizaciones a cumplir con los requisitos normativos mientras se minimiza la exposición a amenazas cibernéticas.

Capa de protección estándar

En el núcleo, nuestra conectividad segura ofrece opciones de red privada cifrada que incluyen VPN IPsec, APN privados, direccionamiento IP privado fijo y bloqueo por IMEI. Estas herramientas trabajan conjuntamente para garantizar la transmisión segura de los datos y un acceso controlado a la red, independientemente de la ubicación de la SIM o del operador.

Controles avanzados e integración

Más allá de la protección básica, nuestro Marco de Seguridad IoT incorpora capacidades avanzadas como la detección de anomalías impulsada por IA, que supervisa continuamente el comportamiento de los dispositivos para identificar patrones irregulares y posibles amenazas en tiempo real. Este enfoque proactivo ayuda a mitigar los riesgos antes de que afecten a la red o a las operaciones.

También somos compatibles con IoT SAFE de la GSMA, lo que permite una seguridad basada en certificados a nivel de hardware al convertir la SIM en una raíz de confianza segura. IoT SAFE facilita la autenticación mutua y el intercambio de datos cifrados entre dispositivos y servicios en la nube, reduciendo la dependencia de infraestructuras de seguridad externas y garantizando una protección resistente a manipulaciones a gran escala.

Principales beneficios para ti

Nuestro Marco de Seguridad IoT garantiza una protección coherente y escalable, adaptada a distintos tipos de dispositivos y entornos de red. Desde la visibilidad y el control en tiempo real hasta el soporte completo para el cumplimiento normativo, las empresas pueden desplegar soluciones IoT con total confianza, sin comprometer su postura de seguridad.

Facilidad y coste de adopción

Con la seguridad integrada en cada SIM y gestionada de forma centralizada, las empresas evitan el coste y la complejidad de combinar soluciones de terceros. Nuestra plataforma unificada permite un aprovisionamiento rápido, actualizaciones flexibles de políticas y un despliegue global fluido, acelerando la adopción segura de IoT a gran escala.



Descubre más sobre Kheiron y por qué deberías asociarte con Wireless Logic.



Operaciones globales 24/7

Ofrecemos operaciones globales 24/7 desde nuestros centros de servicio en Asia, Europa y Norteamérica.

Excelencia en soporte como estándar

SIM Assist es un servicio de tres niveles diseñado para adaptarse a las necesidades y presupuestos de despliegues de IoT locales, regionales y globales. Todos los clientes tienen acceso al asistente digital Wilo. Wilo se basa en IA, ML y NLP para automatizar las solicitudes de servicio rutinarias y liberar a los agentes de soporte para que puedan centrarse en incidencias más complejas y orientadas al cliente.

SIM Assist Enterprise está diseñado para proveedores de soluciones de primer nivel, OEM y grandes empresas con necesidades de soporte global, así como para afrontar los retos más complejos de los despliegues internacionales. Incluye funcionalidades premium como revisiones de servicio trimestrales, acceso 24/7 al soporte técnico de nuestros equipos de Redes y Operaciones y un gestor de atención dedicado.

Principales beneficios para ti

Nuestro equipo de Operaciones Globales 24/7 y los servicios SIM Assist están diseñados para reducir tu coste de propiedad, manteniendo procesos de despliegue ágiles y minimizando los retrasos en la resolución de incidencias. Por ejemplo, nuestro proceso de onboarding incluye pruebas y consultoría de dispositivos para garantizar que funcionen correctamente en campo. Esto asegura un buen rendimiento en roaming, la capacidad de gestión over-the-air (OTA) y el cumplimiento de los requisitos normativos.

Una vez desplegado, tus equipos pueden apoyarse en la experiencia de nuestros equipos de Redes y Operaciones distribuidos a nivel mundial, que ofrecen soporte localizado y en tiempo real para tus despliegues de IoT. El equipo está enfocado en ayudarte a desplegar, escalar y mantener soluciones críticas y de alta disponibilidad.

Facilidad y coste de adopción

Selecciona el nivel de servicio SIM Assist que mejor se adapte a los requisitos de tu proyecto. Los despliegues globales y de misión crítica requieren el nivel de soporte SIM Assist Enterprise.



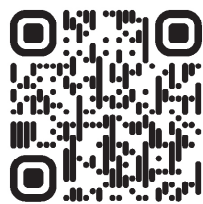
Descubre cómo Wireless Logic puede ayudarte a crear soluciones resilientes y de alta disponibilidad.

Contacto Wireless Logic

Una conectividad fiable y una seguridad robusta son fundamentales para mantener la eficiencia operativa, la productividad, la seguridad y la protección en empresas de todos los sectores. Las normativas gubernamentales y sectoriales exigen un uso cada vez mayor de dispositivos conectados y, además, son cada vez más estrictas en materia de disponibilidad, ciberresiliencia y privacidad de los datos.

Este documento pone de manifiesto el papel clave de los Proveedores de Servicios de Comunicaciones a la hora de ayudarte a cumplir estos requisitos y alcanzar los resultados empresariales deseados mediante IoT.

No esperes al día del despliegue para pensar en la conectividad: planifícala desde el inicio y elige a Wireless Logic como tu socio estratégico de conectividad.



Contáctanos...

para hablar sobre cualquiera de los contenidos de esta guía y recibir un desglose de cómo Wireless Logic aborda los requisitos de alta disponibilidad y ciberresiliencia para empresas que utilizan IoT.





Certificate Number 19387
ISO 9001, ISO 22301, ISO 27001
ISO 14001, ISO 50001

*Thank you for connecting
with Wireless Logic.*

Contact us



Wireless Logic Group Ltd

Horizon, Honey Lane, Hurley, Berkshire SL6 6RJ, UK

Call: +44 (0)330 056 3300

Email: hello@wirelesslogic.com

Web: wirelesslogic.com/conexa

Oficinas

Austria

China

Dinamarca

Francia

Alemania

Italia

Países Bajos

Noruega

España

Reino Unido

Estados Unidos

wirelesslogic.com

