WIRELESS LOGIC **WHITEPAPER**

wireless logic

Maximizar el tiempo de actividad en IoT

Cómo lograr alta disponibilidad y ciberresiliencia en tus despliegues IoT

wirelesslogic.com/es

Por qué los líderes empresariales deberían **preocuparse más por la conectividad**

En un mundo cada vez más conectado, mantener un tiempo de actividad de red sin interrupciones para los dispositivos IoT es más crucial que nunca. El IoT se utiliza en aplicaciones críticas para la seguridad, para optimizar operaciones empresariales, ofrecer servicios innovadores y crear lealtad en los clientes. En todos los casos, una conectividad resiliente es vital y cada vez más exigida por las empresas y los organismos reguladores en todos los sectores de la industria.

Esta guía describe las medidas que deben implementarse en los dispositivos, las redes y los procesos operativos para lograr una alta disponibilidad y resiliencia en el IoT, donde los entornos de telecomunicaciones son complejos, los desafíos del coste de propiedad están en aumento y las amenazas cibernéticas van en aumento.

Infórmate sobre los detalles de implementación que se necesitan en los dispositivos, el entorno en la nube y en la red de tu proveedor de servicios de comunicación para crear resiliencia, una conectividad segura y una recuperación más rápida y automatizada en caso de que ocurra una interrupción.

No trates la conectividad como un coste más de tu negocio. Un servicio de conectividad confiable, seguro y resiliente te ayudará a diferenciarte en el mercado, cumplir con las normas empresariales e industriales y mantenerte fuera del radar de los reguladores.

Regresa al Contenido

Contenido

Regresa al Contenido

Fiabilidad y resiliencia:

Impulsores del mercado y panorama regulatorio

Los organismos de estándares como ISO, ETSI, NIST, junto con las normas de seguridad de la IEC y otras específicas de cada sector, han servido bien a la industria como guías y marcos de buenas prácticas. Ahora, ellos y sus equivalentes globales son obligatorios en la mayoría de los mercados.

A medida que el mundo busca una mayor seguridad, eficiencia energética, menos desperdicio y mejorar los estilos de vida y el bienestar, depende cada vez más de la conectividad. Esto, a su vez, ha creado objetivos para los ciberdelincuentes y ha generado preocupaciones sobre la seguridad de los datos y la privacidad tanto en los consumidores como en las empresas.

Como resultado, los gobiernos han legislado, destacándose la Ley de Ciberresiliencia de la UE, la Ley de Ciberseguridad de China y las Leyes de Seguridad en Telecomunicaciones en EE. UU. y el Reino Unido. Los mercados maduros de Asia-Pacífico (Japón, Corea del Sur, Australia, Singapur, Malasia, Indonesia) y América (Brasil, Canadá, México) tienen leyes equivalentes.

Normas o directivas como ISO 27001, ISO 22301, NIS2, NIST CSF y el RGPD sirven como una buena referencia del panorama global. Con la legislación ya en vigor, estas normas ya no son opcionales.

Ahora imponen requisitos diseñados para asegurar la disponibilidad continua de los dispositivos y redes, la protección y la recuperación rápida ante interrupciones, así como la ciberresiliencia y la privacidad de los datos.

En este documento vamos a ilustrar lo que esto significa para los Proveedores de Servicios de Comunicación y los fabricantes de productos/dispositivos (OEM), Proveedores de Servicios y Empresas.

La Tabla 1 muestra cómo las normas ISO, ETSI, NIST y otras encajan en una estructura general que abarca desde la cadena de suministro y la gestión de riesgos hasta la seguridad de aplicaciones y dispositivos. Todos estos niveles se aplicarán en distintos grados a las soluciones de IoT y todos contribuyen a alcanzar el objetivo de alta disponibilidad. Habrá numerosas regulaciones específicas de sectores o industrias además de las que se mencionan y la guía de GSMA ***Global IoT Regulations*** ofrece una perspectiva complementaria útil.

Las Empresas, los OEM y los Proveedores de Soluciones deben considerar todo este espectro (en la Tabla 1) y diseñar en consecuencia, según sus prioridades de negocio y su actitud frente al riesgo. Al hacerlo, también deben reconocer que el tiempo de inactividad puede deberse a una amplia gama de factores, incluidos fallos o daños electromecánicos, mantenimiento inadecuado, cortes de energía o de red, y ciberataques como infecciones de ransomware o ataques de denegación de servicio a sistemas relacionados.

Más adelante en el documento, examinamos el papel fundamental que desempeñan los proveedores de servicios de comunicación para cumplir con las normas relevantes, ofrecer excelencia operativa y generar diferenciación, utilizando ***Casos prácticos***.

Tabla 1: Ejemplo de estructura de legislación, regulación y normas.

Cadena de Suministro Asegurarte de que los productos y servicios de terceros cumplan con los estándares de seguridad.	ISO/IEC 27036, 28000:2022 NIST 800-161
Gestión de Riesgos Gestionar los riesgos de seguridad y asegurar el cumplimiento de la gobernanza.	ISO/IEC 31000 ISO/IEC 22301 NIST 800-37
Respuesta a Incidentes Marcos para manejar y responder a incidentes de ciberseguridad.	ISO/IEC 27035 NIST 800-61, PCI DSS, GDPR and HIPAA
Seguridad de la nube y la Infraestructura Pautas específicas para asegurar entornos e infraestructura en la nube.	ISO/IEC 27017 Cloud Security Alliance (CSA) STAR Certification NIST SP 800-144
Privacidad de los Datos Regulaciones que rigen la protección de datos personales y los derechos de privacidad.	GDPR, CCPA (California), VCDPA (Virginia) and CPA (Colorado). ISO/IEC 27701
Gestión de la Seguridad Marcos generales de ciberseguridad para la gestión organizacional.	ISO/IEC 27001 NIS2 Directive (EU) NIST CSF
Red Protegiendo la infraestructura de comunicaciones y los datos en tránsito.	ISO/IEC 27033 CRA and NIS2 Directive (EU) NIST CSF
Seguridad de Aplicaciones Estándares y marcos para asegurar software y aplicaciones.	ISO/IEC 27034 NIST 800-53
Seguridad de Dispositivos Foco en hardware, IoT y sistemas embebidos.	ISO/IEC 27002 EU CRA and UK PSTI ETSI EN 303645 NIST CSF US Cyber Trust mark

Regresa al Contenido

Estrategias de proveedores de conectividad para maximizar el tiempo de actividad

Los mejores proveedores de servicios en los ámbitos de la nube, TI e IoT utilizan una combinación de estrategias para asegurar operaciones fiables, seguras y eficientes que maximicen el tiempo de actividad y la resiliencia.

En el espacio del IoT hay dinámicas adicionales que no existen en la misma medida en los entornos de TI más controlados, donde el departamento de TI tiene un control más completo sobre el equipo de red, la conectividad por cable/inalámbrica (ethernet, WiFi), las políticas y los dispositivos (normalmente un pequeño número de equipos de escritorio, portátiles y tabletas aprobados, además de impresoras).

En contraste, el mundo del IoT tiene una enorme cantidad de tipos de dispositivos y tecnologías inalámbricas diferentes. Los dispositivos casi siempre se implementan fuera del dominio de TI, tanto física como virtualmente. Hay menos control sobre las condiciones inalámbricas locales, la congestión o disponibilidad de la red, o el entorno regulatorio y comercial, especialmente en despliegues internacionales.

En IoT es igualmente vital que los OEMs, Proveedores de Soluciones y Empresas adopten el mismo conjunto integral de buenas prácticas y aseguren que se apliquen a nivel de dispositivo, red e infraestructura en la nube. Por supuesto, una parte importante de la solución vendrá de tu Proveedor de Servicios de Comunicación, pero eso no lo es todo, especialmente y más obviamente, a nivel de dispositivo y en tus sistemas empresariales.

Estas prácticas están enumeradas aquí y cubren una variedad de dominios, incluyendo la gestión de infraestructura, la seguridad, los procesos operativos y la comunicación con el cliente. Aquí tienes un resumen de las principales buenas prácticas:

Las mejores prácticas

Para garantizar operaciones fiables, seguras y eficientes, maximizando al mismo tiempo el tiempo de actividad y la resiliencia, los proveedores de servicios de Cloud, TI e IoT deben adoptar las siguientes mejores prácticas:

1. **Resiliencia de la infraestructura:**
   Diseña redes y sistemas con redundancia para evitar puntos únicos de fallo. Usa balanceo de carga y autoescalado para manejar las fluctuaciones en la demanda. Implementa georredundancia y conmutación por error automática para asegurar un servicio continuo, incluso durante interrupciones.
2. **Seguridad:**
   Implementa una Arquitectura Zero Trust con una gestión de identidad y acceso (IAM) sólida, incluyendo autenticación multifactor (MFA) y control de acceso basado en roles (RBAC). Cifra los datos en reposo y en tránsito, realiza análisis de vulnerabilidades de forma regular y usa una protección de endpoints fuerte junto con segmentación de red para mitigar riesgos. Automatiza la gestión de parches para abordar rápidamente las vulnerabilidades.
3. **Recuperación ante desastres:**
   Establece un plan integral de recuperación ante desastres (DR) con copias de seguridad frecuentes usando la estrategia 3-2-1 (3 copias, 2 tipos de medios, 1 fuera del sitio). Prueba los procedimientos de DR regularmente, asegurando una recuperación rápida después de incidentes. Define y cumple con el RTO (Objetivo de Tiempo de Recuperación) y el RPO (Objetivo de Punto de Recuperación) de acuerdo con los SLA.
4. **Monitoreo y mantenimiento predictivo:**
   Usa herramientas de monitoreo y observabilidad en tiempo real para la infraestructura, las aplicaciones y los dispositivos IoT. Aprovecha el análisis predictivo impulsado por IA para anticipar fallos. Centraliza la gestión de registros para detectar problemas más rápido y automatiza las alertas y la gestión de incidentes.
5. **Automatización y coordinación:**
   Usa herramientas de monitoreo en tiempo real y observabilidad para la infraestructura, las aplicaciones y los dispositivos IoT. Aprovecha el análisis predictivo impulsado por IA para anticipar fallos. Centraliza la gestión de registros para detectar problemas más rápido y automatiza las alertas y la gestión de incidentes.
6. **Optimización del rendimiento del servicio:**
   Realiza una planificación de capacidad de forma regular y optimiza el rendimiento utilizando redes de entrega de contenido (CDNs), almacenamiento en caché y computación en el borde para reducir la latencia. Aplica límites de velocidad a las APIs para evitar la sobrecarga y mejorar la eficiencia del sistema.
7. **Gestión de cambios y gobernanza:**
   Utiliza procedimientos formales de control de cambios para reducir los riesgos al implementar actualizaciones. Mantén el control de versiones para las configuraciones y audita los sistemas para asegurar el cumplimiento de estándares regulatorios como el GDPR y la ISO 27001.
8. **Comunicación y soporte al cliente:**
   Proporciona actualizaciones transparentes durante los incidentes a través de páginas de estado y comunicación regular. Ofrece herramientas de autoservicio para que los clientes puedan monitorear sus servicios. Notifica de manera proactiva a los clientes sobre posibles problemas mediante alertas automáticas.
9. **Sostenibilidad:**
   Optimiza el uso de energía en los centros de datos mediante la virtualización, la contenerización y el hardware de bajo consumo. Supervisa el consumo de energía para alinearte con los objetivos de sostenibilidad y reducir la huella ambiental general.

Al aplicar estas prácticas, los proveedores de servicios pueden **asegura altos niveles de tiempo de actividad, seguridad** y **eficiencia operativa**, **mejorando la satisfacción del cliente** y **minimizando las interrupciones del servicio**.

Regresa al Contenido

Estrategias de proveedores de conectividad para maximizar el tiempo de actividad *(continúa)*

Las preguntas clave que debes hacerle a tu proveedor de servicios de comunicación IoT

Basándonos en décadas de experiencia y en la interacción con clientes en procesos formales de RFI y adquisiciones, hemos recopilado una serie de preguntas que deberías hacerle a tu proveedor de servicios de comunicaciones IoT antes de comenzar un nuevo despliegue con ellos.

Estas preguntas específicas te ayudarán a evaluar la ciberresiliencia y la alta disponibilidad (tiempo de actividad) de tu proveedor de servicios de comunicaciones IoT en áreas clave como la seguridad de la infraestructura, la respuesta a incidentes, la disponibilidad del servicio y el cumplimiento normativo.

Infraestructura de Red	¿Cómo aseguras la seguridad de tu infraestructura de comunicaciones?
	¿Qué estándares de cifrado usas para los datos en tránsito y en reposo?
	¿Cómo está segmentada tu red para aislar los datos sensibles del tráfico menos seguro?
	¿Qué protecciones tienes implementadas para mitigar ataques de Denegación de Servicio Distribuido (DDoS)?
	¿Usas firewalls, sistemas de detección/previsión de intrusos (IDS/IPS) o herramientas de monitoreo de red?
	¿Cómo manejas los parches de seguridad y las actualizaciones en toda tu infraestructura?
	¿Qué controles de acceso y de calidad tienes para gestionar y asegurar los dispositivos dentro de tu red?
	¿Con qué frecuencia realizas evaluaciones de vulnerabilidades y pruebas de penetración en tu infraestructura?
Cumplimiento de Normas y Regulaciones	¿Estás certificado bajo algún estándar de la industria como ISO/IEC 27001, CRA/NIS2, TSA, NIST CSF u otros?
	¿Cuál es tu proceso para responder a auditorías e investigaciones regulatorias?
	¿Puedes proporcionar informes de auditoría o evaluaciones de terceros sobre tus prácticas de seguridad (por ejemplo, SOC 2 Tipo II)?
	¿Cómo aseguras que nuestros dispositivos IoT sigan cumpliendo con las regulaciones de GSMA y del Gobierno/Operador local a lo largo del tiempo (por ejemplo, restricciones de roaming permanente)?
Protección de Datos y Privacidad	¿Cómo manejas los datos sensibles o personales (por ejemplo, cifrado, minimización de datos, políticas de retención)?
	¿Dónde se almacenan los datos y están tus centros de datos distribuidos geográficamente para cumplir con los requisitos de residencia de datos?
	¿Cómo aseguras que los datos en tránsito permanezcan dentro de las fronteras regulatorias?
	¿Cómo manejas las transferencias de datos transfronterizas y aseguras el cumplimiento con las leyes de protección de datos en diferentes regiones?
	¿Qué medidas tienes implementadas para prevenir el acceso no autorizado a los datos de los clientes?
	¿Cómo permites que los clientes cumplan con las solicitudes relacionadas con los derechos de los titulares de los datos (por ejemplo, acceso, eliminación, rectificación)?
Respuesta a incidentes y monitorización	¿Tienes un plan documentado de respuesta a incidentes? ¿Puedes compartir los aspectos clave de tu plan?
	¿Cómo detectas y respondes a amenazas cibernéticas o anomalías en la red?
	¿Ofreces monitoreo en tiempo real de los servicios, y qué tipo de alertas reciben los clientes en caso de una violación de seguridad o una interrupción?
	¿Cuál es tu política para reportar incidentes o violaciones de seguridad a los clientes?
	¿Tienes centros de operaciones de seguridad (SOC) dedicados para el monitoreo 24/7 de amenazas potenciales?
	¿Cómo de rápido respondes y mitigas los incidentes de seguridad?
Alta disponibilidad y recuperación ante desastres	¿Cuál es tu tiempo de actividad garantizado (SLA) para los servicios de comunicación?
	¿Qué mecanismos de redundancia y conmutación por error tienes implementados para asegurar una alta disponibilidad?
	¿Cómo aseguras la continuidad del servicio en caso de un desastre natural, corte de energía, interrupción de red o ciberataque?
	¿Cuál es tu plan de recuperación ante desastres y con qué frecuencia lo pruebas?
	¿Tienes centros de datos geográficamente diversos para prevenir tiempos de inactividad debido a interrupciones locales?
	¿Cómo priorizas la recuperación en caso de un fallo o ciberataque?
Flexibilidad y escalabilidad	¿Cómo te aseguras de que tu infraestructura de red pueda soportar las futuras demandas de escalabilidad en términos de conexiones de dispositivos IoT, volumen de datos y latencia?
Respaldo y retención de datos	¿Cuál es tu estrategia de backup para los datos de comunicación, y con qué frecuencia se realizan los backups?
	¿Cómo aseguras que los datos respaldados estén seguros (por ejemplo, mediante cifrado y control de acceso)?
	¿Cuánto tiempo retienes los datos de los clientes, y pueden los clientes configurar las opciones de retención de datos para cumplir con sus políticas internas?
	¿Cómo manejas la restauración de los datos respaldados en caso de un fallo del sistema?
Gestión de riesgos de terceros	¿Confías en algún proveedor externo para tus servicios, y cómo verificas sus prácticas de seguridad?
	¿Cómo te aseguras de que tus proveedores externos cumplan con tus estándares de ciberseguridad y disponibilidad?
	¿Qué acuerdos contractuales tienes con tus proveedores externos en cuanto a la seguridad y la disponibilidad del servicio?

Regresa al Contenido

Estrategias de proveedores de conectividad para maximizar el tiempo de actividad *(continúa)*

Gestión del cambio y actualizaciones de servicio	¿Cuál es tu proceso para implementar actualizaciones o cambios en tu infraestructura?
	¿Cómo notificas a los clientes sobre el mantenimiento programado o los cambios que podrían afectar el servicio?
	¿Cómo se prueban las actualizaciones antes de implementarlas en los entornos de producción?
	¿Cómo manejas el tiempo de inactividad no planificado o las actualizaciones de emergencia, y cuáles son tus procedimientos de comunicación?
Control del cliente y transparencia	¿Qué nivel de control tienes sobre la configuración y los ajustes de seguridad de los servicios que te ofrecemos?
	¿Te damos visibilidad de nuestras medidas de seguridad y del estado de la red a través de paneles o informes regulares?
	¿Puedes realizar tus propias auditorías o evaluaciones de nuestra infraestructura y medidas de seguridad?
	¿Ofrecemos formación o recursos sobre concienciación en seguridad para ti como cliente?
Métricas de rendimiento e informes	¿Qué métricas clave de rendimiento (KPIs) sigues para garantizar la fiabilidad del servicio y la seguridad?
	¿Cómo informas sobre el rendimiento del sistema y qué nivel de detalle se proporciona a los clientes?
	¿Pueden los clientes acceder a datos en tiempo real e históricos sobre el rendimiento, incidentes y caídas del servicio?
Soporte al final de la vida útil y migración	¿Cómo manejas el soporte al final de la vida útil para tecnologías o servicios obsoletos?
	¿Cuál es tu plan para migrar a los clientes a nuevas tecnologías o plataformas con una mínima interrupción?
	¿Cómo aseguras que se mantenga la seguridad durante las migraciones o actualizaciones?
Implicaciones de costes de la ciberresiliencia	¿Cuáles son los costes asociados con garantizar alta disponibilidad, seguridad y cumplimiento?
	¿Hay tarifas adicionales por servicios de seguridad premium o acuerdos de nivel de servicio (SLA) extendidos?
	¿Ofreces soluciones escalables para ciberseguridad y disponibilidad según el tamaño del cliente y el nivel de riesgo?
Sostenibilidad empresarial y hoja de routa	Por favor, proporciona información detallada sobre la salud financiera de tu empresa y su viabilidad a largo plazo, incluyendo, pero no limitándose a, ingresos, rentabilidad, estrategia financiera a largo plazo y actividad de fusiones y adquisiciones (M&A).
	Por favor, proporciona detalles sobre la inversión de tu empresa en Investigación y Desarrollo (I+D), incluyendo el porcentaje de los ingresos anuales que se ha destinado a I+D en los últimos tres años y cómo el gasto en I+D de tu empresa se alinea con su estrategia de innovación a largo plazo.
	Describe iniciativas o proyectos destacados de I+D que contribuyan directamente a mejorar tu oferta de servicios, incluyendo, pero no limitándose a, 5GSA, eRedCap, IPv6, distribución de pasarelas de paquetes (Packet Gateway), ciberresiliencia, asociaciones con operadores, aprovisionamiento remoto de SIM, eSIM e iSIM.

Estas preguntas se han recopilado a partir de reuniones con analistas, consejos de consultores y procesos de solicitud de información por parte de clientes, y ofrecen una evaluación completa de la capacidad del proveedor de servicios de comunicaciones para ofrecer ciberseguridad robusta, proteger activos críticos y mantener altos niveles de disponibilidad del servicio. Además, ayudan a evaluar si el proveedor cuenta con las políticas, la infraestructura y el compromiso adecuados para cumplir con los estándares de la industria y los requisitos de cumplimiento normativo.

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 las empresas que utilizan IoT.

Regresa al Contenido

Estrategias de proveedores de conectividad para maximizar el tiempo de actividad *(continúa)*

¿Por qué la conectividad celular es la tecnología más resiliente?

Al comparar diferentes tecnologías inalámbricas, es importante considerar el conjunto más amplio de factores involucrados en la elección tecnológica. Con ese fin, la Tabla 2 resume algunas de las diferencias clave entre tecnologías inalámbricas populares junto con los criterios de resiliencia. Bluetooth Low Energy (BTLE) tiene una baja resiliencia, pero también ha demostrado ser una solución perfectamente válida para ciertos casos de uso en el hogar o el automóvil.

Para la mayoría de las aplicaciones del Internet de las Cosas (IoT) y muchas aplicaciones empresariales, las tecnologías celulares serán la opción más resiliente y confiable para aplicaciones críticas que requieren una comunicación constante y segura, especialmente en entornos dinámicos o impredecibles.

1 **Cobertura amplia y ubicuidad**
Las redes celulares ofrecen una cobertura extensa, que a menudo abarca vastas áreas geográficas, incluidas zonas remotas o de difícil acceso.

2 **Ecosistema e interoperabilidad**
Las redes celulares están basadas en estándares globales bien establecidos, desarrollados por organizaciones como el 3rd Generation Partnership Project (3GPP) y la GSMA, para asegurar un alto grado de interoperabilidad entre dispositivos y redes a nivel mundial. El ecosistema de proveedores de servicios de comunicaciones es un grupo amplio que incluye operadores móviles (MNO) y operadores móviles virtuales (MVNO), lo que te da opciones y facilita el cambio de proveedor gracias a la provisión remota de SIM.

3 **Infraestructura redundante**
Las redes celulares están construidas con alta redundancia y múltiples capas de mecanismos de recuperación ante fallos. Los operadores de telecomunicaciones suelen utilizar estaciones base redundantes, conexiones de backhaul y otros elementos de infraestructura para garantizar el funcionamiento continuo en caso de fallos de hardware, desastres naturales o cortes localizados.

4 **Protocolos de seguridad robustos**
Las redes celulares utilizan protocolos de seguridad avanzados, como la autenticación basada en SIM y estándares de cifrado fuertes (por ejemplo, cifrado 3GPP, IPsec para backhaul celular), para proteger las comunicaciones. Esto añade una capa de ciberresiliencia, reduciendo el riesgo de accesos no autorizados y ataques que podrían comprometer otras tecnologías inalámbricas.

5 **Sistemas de backup energéticos altamente confiables**
Las torres celulares están equipadas con sistemas de respaldo de energía (como baterías o generadores), lo que les permite seguir funcionando durante apagones o interrupciones en la red eléctrica. Esto asegura que la conectividad se mantenga incluso durante emergencias, cuando otras formas de conectividad, como wifi o fibra óptica, pueden fallar.

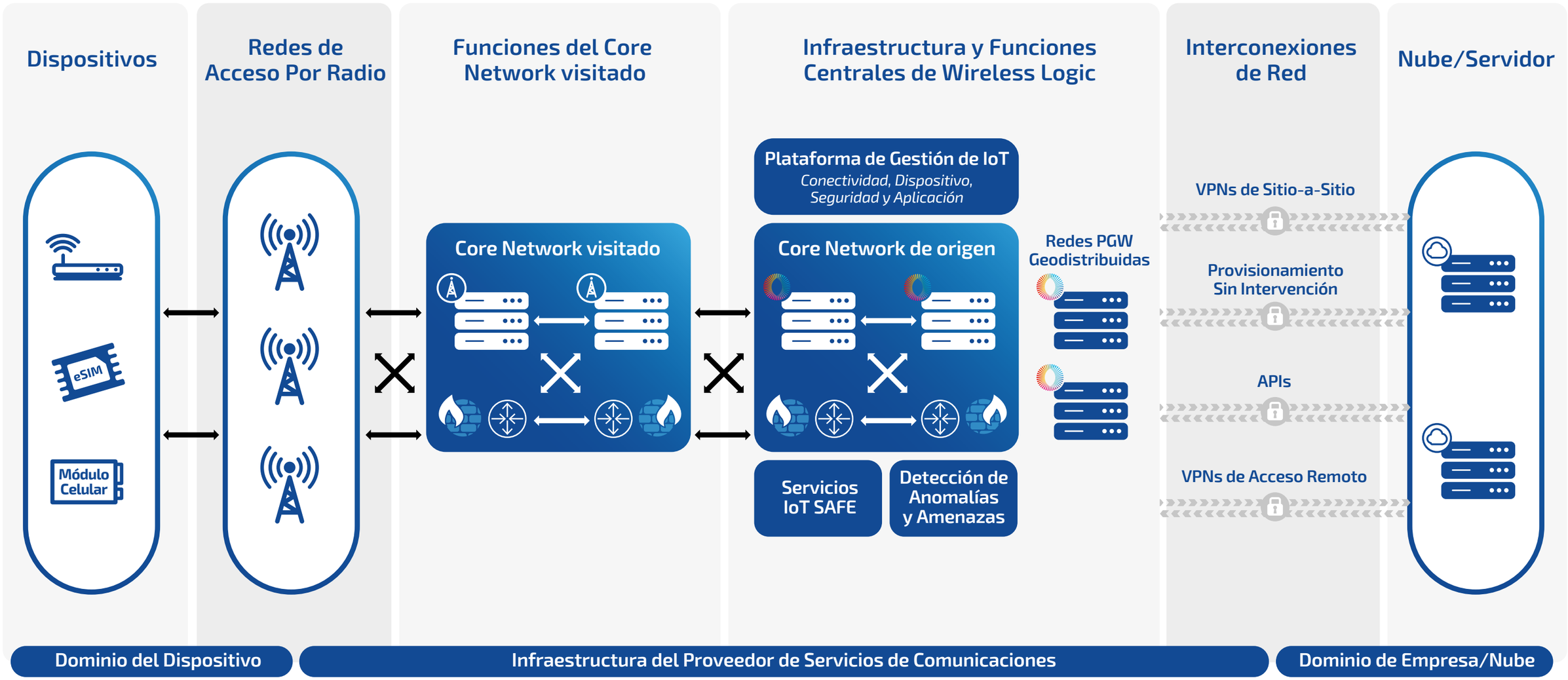
6 **Capacidades de movilidad y roaming**
Las redes celulares proporcionan movilidad sin interrupciones y capacidades de roaming, permitiendo que los dispositivos permanezcan conectados mientras se desplazan entre regiones o redes. Esto es especialmente importante para dispositivos IoT, vehículos o activos en movimiento, ya que garantiza conectividad continua a través de fronteras o zonas de cobertura celular sin necesidad de reconfiguración manual.

Tabla 2: Resumen de las principales diferencias en tecnologías inalámbricas

	Alcance	Eficiencia energética	Ancho de banda	Mejor caso de uso	Latencia	Topología de red	Seguridad	Resiliencia	
BTLE	Corto *(~100 m)*	Muy Alta	Bajo	Personal, Dispositivos portátiles	Muy Baja	Punto-a-punto	AES-128	Limitada	*Resiliencia limitada debido al corto alcance y la susceptibilidad a interferencias en entornos concurridos.*
Zigbee	Corto *(~10-100 m)*	Muy Alta	Bajo	Hogar, Edificios	Muy Baja	Malla	AES-128	Moderada *(La red en malla añade redundancia)*	*La topología de red en malla mejora la resiliencia porque los datos pueden redirigirse si un nodo falla, aunque la resiliencia general depende de la densidad de los nodos.*
WiFi	Medio *(~100 m - 1 km)*	Moderada	Alto	Hogar, Oficina	Baja	Estrella o Malla	WPA2/WPA3	Moderada	*Moderada, dependiente de la configuración de la red. Vulnerable a interferencias, fallos del router y congestión de la red.*
LoRaWAN	Largo *(up to 15 km)*	Ultra-Alta	Bajo	Remoto, Ciudad, Campus	Baja	Estrella	AES-128	Alta	*Alta resiliencia debido a su capacidad para operar en redes de largo alcance y bajo consumo de energía. Los dispositivos LoRaWAN pueden seguir funcionando durante períodos prolongados en ubicaciones remotas sin depender de infraestructuras que consumen mucha energía.*
Cellular	Muy Largo *(national/global)*	Moderada a Alta	Moderado a Alto	Gama versátil de aplicaciones fijas, móviles y en tiempo real	Baja a Moderada	Estrella	Autenticación basada en SIM, cifrado de nivel operador	Muy Alta	*Alta resiliencia, con infraestructura robusta, múltiples sistemas de conmutación por error y sólidas prácticas de gestión de redes.*
Satellite	Global, incluyendo zonas remotas	Baja *(Improving with LEO and NTN)*	Moderado a Alto	Remoto Recuperación ante desastres Seguimiento marítimo global	Alta *(debido a la distancia del satélite)*	Estrella	Cifrado fuerte	Muy Alta	*Las redes satelitales son extremadamente resistentes, especialmente en escenarios de desastre, lugares remotos o áreas donde la infraestructura terrestre está dañada o no disponible.*

De un vistazo:

Creando confiabilidad, resiliencia y seguridad de extremo a extremo para el IoT



Capacidades Avanzadas de Red y SIM

En detalle:

Creando confiabilidad, resiliencia y seguridad de extremo a extremo para el IoT

En el espacio del Internet de las Cosas (IoT), hay dinámicas y variables adicionales que no existen en la misma medida en los entornos de IT más controlados, donde el departamento de IT tiene un control más completo. Con el IoT, hay una enorme cantidad de tipos de dispositivos y entornos de redes inalámbricas que están fuera del alcance del CISO, CIO y del perímetro de IT.

Vulnerabilidades en el dominio del dispositivo y de la red de acceso radioeléctrico.

La tecnología celular tiene un largo historial de resiliencia y fiabilidad, pero como ocurre con todas las tecnologías inalámbricas, puede verse afectada por factores ambientales y técnicos que casi siempre son temporales, y cuyas implicaciones pueden variar según la aplicación. A continuación, se describen las posibles fuentes de pérdida de conectividad en una Red de Acceso Radio (RAN).

Los sistemas que dependen de la comunicación en tiempo real, críticos para la seguridad o el negocio, como la infraestructura crítica, el monitoreo de salud, los vehículos autónomos o la automatización industrial, deberán ser diseñados en consecuencia tanto a nivel de dispositivo como de sistema. Otros sistemas IoT que se utilizan en situaciones de monitorización más pasiva puede que ni siquiera se vean afectados.

1. **Cobertura de red y fuerza de la señal**
   Diseña sistemas con redundancia para evitar puntos únicos de falla. Usa balanceo de carga y escalamiento automático para manejar fluctuaciones en la demanda. Implementa georredundancia y conmutación por error automática para asegurar un servicio continuo, incluso durante interrupciones.

2. **Interferencia**
   La interferencia electromagnética (EMI) causada por maquinaria industrial, líneas eléctricas o dispositivos electrónicos, y la interferencia por radiofrecuencia (RFI) de sistemas de comunicación cercanos, puede degradar las señales celulares. Esto es particularmente problemático en entornos industriales o en áreas urbanas densamente pobladas, donde múltiples dispositivos transmiten señales simultáneamente. La presencia de torres celulares cercanas que operan en frecuencias similares también puede provocar degradación de la señal, causando problemas de conectividad en los dispositivos IoT.

3. **Congestión de la red**
   La congestión de red ocurre cuando muchos dispositivos intentan conectarse a la misma torre celular, especialmente durante los momentos de mayor uso o en zonas de alta densidad. Esta congestión puede saturar la red, provocando una transmisión de datos más lenta, mayor latencia o desconexiones. Los dispositivos IoT, especialmente aquellos que requieren datos en tiempo real, pueden experimentar retrasos significativos o pérdida de conectividad cuando la red está congestionada.

4. **Fenómenos meteorológicos extremos y desastres naturales**
   Las condiciones climáticas severas como lluvias intensas, tormentas de nieve, rayos o vientos fuertes pueden atenuar las señales, especialmente en bandas de frecuencia más altas como 5G. Los desastres naturales como huracanes, inundaciones y terremotos pueden dañar infraestructura celular crítica, incluidas torres y cables subterráneos, causando interrupciones generalizadas. Durante estos eventos, incluso los dispositivos IoT más resilientes pueden perder conectividad al verse afectada la infraestructura de red que los respalda.

5. **Construcción y cortes de energía**
   Las actividades de construcción representan otro riesgo, ya que los trabajadores pueden dañar sin querer infraestructura celular como cables de fibra óptica subterráneos. Además, las barreras temporales de construcción pueden obstruir las señales inalámbricas, degradando la calidad de la conexión. Los cortes de energía, causados por tormentas o accidentes, pueden dejar fuera de servicio torres celulares y otros equipos de red, generando problemas significativos de conectividad para los dispositivos IoT que dependen de una comunicación continua.

Mitigar estos riesgos implica una planificación proactiva, un diseño sólido de la SIM, del dispositivo, del sistema y de las aplicaciones, una infraestructura de red resiliente y la incorporación de sistemas de respaldo para asegurar una **conectividad constante y confiable de los dispositivos IoT en diversos entornos.**

Regresa al Contenido

En detalle:

Creando confiabilidad, resiliencia y seguridad de extremo a extremo para el IoT *(continúa)*

Capacidades obligatorias de los dispositivos IoT para alta disponibilidad y ciberresiliencia

Ya seas un fabricante (OEM), proveedor de soluciones o usuario empresarial, la alta disponibilidad y la ciberresiliencia en dispositivos IoT solo se pueden lograr implementando una serie de medidas de seguridad, confiabilidad y redundancia como las que se detallan a continuación. No basta con confiar únicamente en las capacidades de tus proveedores de comunicaciones o servicios en la nube; las capacidades del dispositivo y cómo se comporta en la red son igual de importantes.

Los dispositivos IoT suelen estar muy distribuidos y operar en entornos diversos, lo que los hace particularmente vulnerables a amenazas cibernéticas y posibles tiempos de inactividad. Además, a menudo tienen limitaciones de costo o recursos, lo que significa que inevitablemente habrá que hacer compromisos respecto a las mejores prácticas. Haz esos compromisos de forma cuidadosamente pensada.

Usa nuestra guía para crear especificaciones de requisitos y como marco de referencia para esas decisiones de diseño.

Arranque Seguro e Integridad del Firmware	**Arranque seguro:** Implementa mecanismos de arranque seguro para asegurarte de que solo el firmware confiable, firmado y autenticado pueda ejecutarse en el dispositivo. Esto evita que se inyecte código malicioso en el proceso de arranque. **Autenticación del Dispositivo y Gestión de Identidad** **Actualizaciones Over-the-air (OTA):** Proporciona mecanismos seguros para actualizaciones OTA con la debida encriptación, autenticación y verificación, para mantener los dispositivos actualizados contra vulnerabilidades conocidas.
Autenticación de Dispositivos y Gestión de Identidad	**Identidad única del dispositivo:** Asegúrate de que cada dispositivo IoT tenga una identidad única e inmutable para evitar suplantaciones o imitaciones. **Autenticación mutua:** Implementa protocolos de autenticación mutua (por ejemplo, certificados X.509 o Infraestructura de Clave Pública, PKI) para establecer confianza entre los dispositivos y los servidores. **Raíz de confianza en hardware (RoT):** Utiliza seguridad basada en hardware, como el Módulo de Plataforma Confiable (TPM) o el Elemento Seguro (SE), para proporcionar una raíz de confianza en hardware para operaciones criptográficas e identidad del dispositivo.
Diseño y posicionamiento de antenas	**El diseño y la colocación de la antena son fundamentales para mantener una conectividad de alta disponibilidad en los dispositivos IoT.** Un diseño adecuado garantiza una señal óptima y buena cobertura, mientras que una colocación estratégica minimiza las interferencias y los obstáculos en la señal. Una ubicación efectiva de la antena mejora la fiabilidad, reduce la pérdida de conexión y mejora el rendimiento general, especialmente en entornos difíciles o lugares remotos.
Cifrado de datos	**Cifrado de datos en reposo:** Usa algoritmos de cifrado fuertes (por ejemplo, AES-256) para cifrar los datos sensibles almacenados en el dispositivo, evitando el acceso no autorizado si el dispositivo se ve comprometido. **Cifrado de datos en tránsito:** Asegura los canales de comunicación usando protocolos de cifrado a nivel de transporte como TLS/SSL para proteger los datos transmitidos entre dispositivos y redes. **Cifrado de extremo a extremo:** Asegúrate de que los datos permanezcan cifrados desde el punto de recolección hasta el destino final, reduciendo la exposición a ataques de intermediarios (MITM).
Comunicación de red resiliente	**Canales de comunicación redundantes:** Tarjetas SIM multi-red y multi-IMSI y/o soluciones eSIM, iSIM para maximizar tu control y la capacidad de cambiar entre infraestructuras de diferentes proveedores de red. **Mecanismos de respaldo y conmutación por error:** Usa sistemas de conmutación por error de red para asegurar la disponibilidad continua del servicio en caso de interrupciones. **Segmentación de red:** Asegúrate de que los dispositivos IoT operen en redes segmentadas, aislando los dispositivos críticos y limitando su exposición a otros sistemas vulnerables dentro de la red.
Monitoreo en tiempo real y detección de amenazas	**Sistemas de detección y prevención de intrusiones (IDPS):** Integra capacidades IDPS incorporadas que puedan detectar anomalías en tiempo real y prevenir acciones maliciosas como accesos no autorizados o ataques de denegación de servicio (DoS). **Monitoreo de registros:** Activa el registro detallado en los dispositivos IoT para monitorear y registrar eventos del sistema, incidentes de seguridad y datos de rendimiento, los cuales pueden analizarse para una detección proactiva de amenazas. **Monitoreo de salud:** Incluye funciones para el monitoreo en tiempo real del estado del dispositivo, como el uso de CPU, consumo de memoria, latencia de red, temperatura y otros indicadores críticos de rendimiento, para asegurarte de que los dispositivos estén funcionando de forma óptima.

Regresa al Contenido

En detalle:

Creando confiabilidad, resiliencia y seguridad de extremo a extremo para el IoT *(continúa)*

Mecanismos a prueba de fallos y redundancia	**Componentes de Hardware Redundantes:** Cuando sea posible, diseña los dispositivos con componentes de hardware redundantes (por ejemplo, fuentes de alimentación duales o rutas de comunicación redundantes) para evitar puntos únicos de fallo.
	Degradación Controlada: Asegúrate de que los dispositivos IoT puedan seguir funcionando en un modo degradado si algunos componentes fallan, permitiendo que las funciones esenciales continúen.
	Fuente de energía de backup: Incluye fuentes de energía de respaldo, como baterías o tecnologías de recolección de energía, para asegurar un funcionamiento ininterrumpido durante cortes de electricidad.
Gestión de parches y actualizaciones de vulnerabilidades	**Actualizaciones regulares de firmware:** Establece un proceso sólido para entregar parches de firmware seguros y puntuales que aborden vulnerabilidades de seguridad.
	Actualizaciones automáticas: Siempre que sea posible, implementa mecanismos de actualización automática que no dependan de la intervención del usuario para reducir el riesgo de que queden vulnerabilidades sin corregir.
	Mecanismo de reversión de actualizaciones: Proporciona la capacidad de revertir actualizaciones de firmware si surge un problema durante o después del parche, asegurando una mínima interrupción en la disponibilidad del servicio.
Control de acceso a dispositivos	**Control de acceso basado en roles (RBAC):** Implementa un control de acceso basado en roles o privilegios para limitar qué usuarios o sistemas pueden interactuar con el dispositivo, minimizando la superficie de ataque.
	Autenticación multifactor (MFA): Incorpora autenticación multifactor para acceder a las interfaces de gestión del dispositivo y evitar accesos no autorizados.
	Principio de mínimo privilegio: Diseña el software y firmware del dispositivo siguiendo el principio de mínimo privilegio, asegurando que cada servicio o componente tenga solo el nivel mínimo de acceso necesario para funcionar.
Resistencia a ataques físicos	**Detección de manipulación:** Incorpora mecanismos de detección de manipulación que activen alarmas o borren datos sensibles si el dispositivo es manipulado físicamente.
	Cubierta de hardware segura: Utiliza carcasas seguras y resistentes a manipulaciones para proteger los componentes internos contra accesos no autorizados o ataques de hardware (por ejemplo, puertos JTAG o de depuración). Idealmente, elige SIMs integradas y elimina las ranuras para tarjetas SIM extraíbles.
Gestión del ciclo de vida del dispositivo y de los datos	**Desmantelamiento seguro:** Proporciona procedimientos seguros de desmantelamiento para asegurarte de que los datos sensibles se borren de forma segura cuando el dispositivo llegue al final de su vida útil.
	Políticas de retención de datos: Implementa políticas de retención de datos configurables que permitan a las organizaciones controlar cuánto tiempo se almacenan los datos en el dispositivo antes de ser eliminados.
	Recuperación del dispositivo: Permite que los dispositivos se recuperen automáticamente de estados de fallo (por ejemplo, temporizadores watchdog) y vuelvan a un modo operativo seguro, minimizando el tiempo de inactividad.
Cumplimiento de normas y regulaciones del sector	**Sigue GSMA TS.34:** Sigue las directrices de eficiencia de conexión para dispositivos IoT de GSMA TS.34 para asegurarte de que los dispositivos se comporten adecuadamente en la red y no generen señalización innecesaria ni desperdicien sus propios recursos energéticos.
	Asegúrate de que los dispositivos cumplan con las normas ISO, NIST y ETSI apropiadas para la seguridad de datos y ciberseguridad.
Pruebas y garantía de calidad (por ejemplo, TUV, UL)	**Pruebas de penetración:** Realiza pruebas de penetración periódicas en los dispositivos para identificar posibles vulnerabilidades que los hackers podrían explotar.
	Pruebas de estrés: Lleva a cabo pruebas de estrés para evaluar la capacidad del dispositivo de mantener su funcionalidad bajo condiciones de alta carga o durante cortes de red.
	Certificación: Busca la certificación de autoridades de seguridad de confianza para validar la seguridad y disponibilidad de los dispositivos IoT.

Regresa al Contenido

En detalle:
Creando confiabilidad, resiliencia y seguridad de extremo a extremo para el IoT *(continúa)*

Alta disponibilidad mediante computación en el borde y descentralización	**Computación de borde:** Desvía el procesamiento crítico al borde (puertas de enlace locales) para minimizar la latencia y asegurar el funcionamiento incluso cuando el servicio en la nube no esté disponible. **Almacenamiento de datos centralizado:** Implementa arquitecturas de almacenamiento de datos descentralizadas (por ejemplo, blockchain o tecnologías de registro distribuido) para garantizar la integridad y disponibilidad de los datos incluso si se compromete un servidor central.
Seguridad desde el diseño y privacidad desde el diseño	**Seguridad desde el diseño:** Integra la seguridad en el proceso de diseño y desarrollo de los dispositivos IoT, teniendo en cuenta los riesgos de ciberseguridad en cada etapa. **Privacidad desde el diseño:** Asegúrate de que las consideraciones de privacidad (como la minimización de datos y la anonimización) estén integradas durante el desarrollo del dispositivo IoT para cumplir con normativas como el RGPD.
Seguridad de componentes de terceros	**Verificación de componentes de terceros:** Asegúrate de que cualquier componente de terceros (hardware o software) incluido en el dispositivo esté debidamente verificado para detectar vulnerabilidades de seguridad y se actualice con regularidad. **Seguridad en la cadena de suministro:** Implementa controles de seguridad rigurosos en toda la cadena de suministro para evitar que componentes manipulados o maliciosos se integren en el producto final.

Al implementar estas medidas, los fabricantes de equipos originales (OEMs) pueden asegurarse de que sus **dispositivos IoT sean altamente disponibles y ciberresilientes**, ayudando a las organizaciones a mitigar riesgos, garantizar una operación continua y cumplir con las regulaciones de la industria. Estos principios también ayudan a **mejorar la confianza y la seguridad que los clientes tienen** en la fiabilidad y protección de los productos IoT.

Capacidades avanzadas del dispositivo, la red y la SIM para una alta disponibilidad y ciberresiliencia.

En la página 8 documentamos una amplia lista de preguntas específicas diseñadas para ayudarte a evaluar la ciberresiliencia y la alta disponibilidad de un proveedor de servicios de comunicaciones IoT.

Si quieres ver una respuesta de Wireless Logic a cada una de las preguntas listadas, puedes solicitarlo a través de *Contáctanos*.

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 las empresas que usan IoT.

En las siguientes secciones, resumiremos algunas de las principales directrices para dispositivos y soluciones que Wireless Logic implementa en nuestras propias redes y con nuestros clientes para optimizar la alta disponibilidad y la ciberresiliencia.

Qué deben hacer los dispositivos si ocurren interrupciones para protegerse y asegurar una recuperación adecuada.

Capacidades avanzadas de red y SIM que te ayudarán a lograr el cumplimiento normativo y la diferenciación.

Regresa al Contenido

En detalle:

Creando confiabilidad, resiliencia y seguridad de extremo a extremo para el IoT *(continúa)*

Qué deben hacer los dispositivos si ocurren interrupciones para protegerse y asegurar una recuperación adecuada.

El documento de la GSMA ***TS.34 - IoT Device Connection Efficiency Guidelines*** proporciona un conjunto extenso de pautas de buenas prácticas para dispositivos IoT y debe ser seguido por los desarrolladores de dispositivos IoT.

En escenarios de IoT, el firmware y el software del dispositivo IoT juegan un papel importante en el rendimiento general y el comportamiento del sistema IoT en su conjunto, incluido el impacto en la red celular. Al no haber intervención humana a la que recurrir, los mecanismos que gestionan el arranque y cómo se comportan los dispositivos al entrar y salir de cobertura o al recuperarse de una interrupción deben estar integrados en el diseño de los dispositivos IoT.

Los 8 pasos a continuación se centran en esas etapas de recuperación que ayudan a garantizar la integridad de los datos, minimizar el consumo de energía y restaurar la conexión de manera eficiente y sin sobrecargar la red en recuperación.

Usa nuestra guía para crear especificaciones de requisitos y como marco para tomar decisiones de diseño.

Detecta la pérdida de red *Haz una distinción entre un evento de interrupción o una pérdida temporal de conexión causada por un cambio de ubicación y la pérdida de cobertura.*	**Monitorización regular:** El dispositivo debe monitorear continuamente su estado de conexión revisando señales de red, pérdida de mensajes de latido (heartbeat) o la falta de confirmaciones del servidor.	**Tiempos de espera y reintentos:** Implementa un mecanismo de tiempo de espera para definir cuánto tiempo espera el dispositivo antes de considerar una falla de comunicación. Al expirar el tiempo, inicia una cantidad predefinida de intentos de reconexión.
Apagado gradual de funciones no críticas	**Almacenamiento temporal de datos:** Antes de apagarse o cambiar al modo de bajo consumo, el dispositivo debe guardar localmente cualquier dato no enviado (en memoria no volátil si es posible). Esto asegura que no se pierdan datos críticos durante la interrupción.	**Prioriza tareas:** Suspende funciones no esenciales como el envío de actualizaciones periódicas de estado o telemetría menos crítica, mientras que las funciones críticas como el monitoreo de sensores deben seguir operando y almacenando datos.
Cambia al modo de bajo consumo	**Conservación de energía:** Para extender la vida útil de la batería durante una interrupción de red, el dispositivo debe cambiar a un modo de bajo consumo (por ejemplo, sueño profundo o modo inactivo). Esto reduce el consumo de energía mientras se mantiene listo para cuando la red vuelva a estar disponible.	**Despertar programado:** El dispositivo debe activarse periódicamente en intervalos definidos para intentar reconectarse, asegurando que no permanezca en modo de bajo consumo indefinidamente.
Reintenta los intentos de conexión	**Retroceso exponencial:** Implementa un algoritmo de retroceso exponencial para gestionar los intentos de reconexión. Después de cada intento fallido, el dispositivo debería aumentar el tiempo entre intentos (por ejemplo, 2 segundos, 4 segundos, 8 segundos, etc.), evitando así un consumo excesivo de batería y reduciendo la carga en la red.	**Supervisa la intensidad de la señal:** Antes de reintentar una conexión, el dispositivo debe comprobar la intensidad de la señal de red para asegurarse de que las condiciones son favorables. Intentar reconectar con una señal débil puede provocar un consumo excesivo de energía.
Cambia a redes alternativas *(Si están disponibles)*	**Enviar alertas:** Si es posible antes de la pérdida total de comunicación, el dispositivo debería notificar al servidor o a la plataforma en la nube sobre la pérdida inminente de la red, para que el sistema pueda tomar medidas apropiadas, como marcar el dispositivo como fuera de línea o cambiar la lógica de procesamiento de datos.	**Estrategia de cambio:** Define una estrategia para cómo el dispositivo cambia entre redes primarias y secundarias, incluyendo las condiciones para volver a la red primaria una vez que se haya restablecido.
Alerta a la gestión del dispositivo y/o a la nube/aplicación *(Cuando sea posible)*	**Enviar alertas:** Si es posible antes de la pérdida total de comunicación, el dispositivo debería notificar al servidor o a la plataforma en la nube sobre la pérdida inminente de la red, para que el sistema pueda tomar medidas apropiadas, como marcar el dispositivo como fuera de línea o cambiar la lógica de procesamiento de datos.	**Activación del modo sin conexión:** La nube puede marcar el dispositivo como 'sin conexión' o 'desconectado' hasta que se vuelva a conectar con éxito, asegurando la consistencia de los datos y evitando errores en la comunicación.
Recuperación automática y resincronización	**Restablecer conexión:** Una vez que la red se haya restaurado, el dispositivo debería restablecer automáticamente la conexión con el servidor o la plataforma en la nube.	**Re-sincronización de datos:** El dispositivo debe subir cualquier dato almacenado en búfer recogido durante la interrupción y sincronizar su reloj y estado con el servidor para asegurarse de que todas las marcas de tiempo y estados del sistema estén alineados.
Manejo de errores alternativo	**Establecer límites de tiempo para interrupciones:** Si la interrupción persiste más allá de un límite predefinido, el dispositivo debería escalar el problema, ya sea cambiando a un método de comunicación de respaldo (si está disponible) o generando alertas para que intervengas.	**Acciones locales:** En caso de una interrupción prolongada, el dispositivo debe tener acciones locales predefinidas para gestionar sus funciones críticas de forma independiente, como registrar datos de sensores, emitir alertas locales o mantener controles ambientales.

Concéntrate en las capacidades avanzadas de red y SIM que te ayudarán a lograr el cumplimiento y la diferenciación.

- **eSIM, iSIM y Aprovisionamiento Remoto de SIM**
- **Autenticación de Dispositivos y Gestión de Identidad**
- **Redes Privadas Seguras**
- **Core Network de Alta Disponibilidad**
- **Plataforma de Gestión de IoT**
- **Detección de Anomalías y Amenazas**
- **Operaciones Globales 24/7**

De un vistazo: Arquitectura del sistema

Regresa al Contenido

eSIM, iSIM y Aprovisionamiento Remoto de SIM (RSP)

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

Los beneficios de seguridad física y fiabilidad que ofrecen las eSIMs integradas y las iSIMs proporcionan una ventaja significativa frente a las tarjetas SIM extraíbles. Para aprovechar al máximo esta ventaja, los fabricantes (OEMs), proveedores de soluciones y empresas también deben aprovechar la Aprovisionamiento Remoto de SIMs (RSP) para gestionar todo el ciclo de vida de la SIM, desde la fábrica hasta el campo.

Solución estándar

Nuestra solución estándar de SIM es un perfil SIM multi-IMSI implementado en una eSIM, lo que proporciona la máxima flexibilidad. El perfil predeterminado siempre está diseñado para ofrecer la mayor cobertura y resiliencia, lo que puede significar 3 o 4 redes por país en los mercados clave. La tecnología multi-IMSI y eSIM permite que se realicen actualizaciones y localizaciones mediante actualizaciones por aire (OTA).

Los principales beneficios para ti

RSP ayuda a las empresas a mantener un alto nivel de cobertura y resiliencia a lo largo del tiempo, y permite realizar cambios a nivel de red o de SIM por aire para resolver problemas de rendimiento, calidad o costes en caso de que surjan. El aumento de restricciones gubernamentales o de operadores sobre el roaming permanente hace que RSP sea esencial para las empresas que operan a nivel internacional.

Opciones de personalización y funciones avanzadas

La capacidad de descargar y cambiar IMSI y perfiles SIM por OTA te da flexibilidad y opciones de personalización que pueden adaptarse a las necesidades de tu negocio y despliegue. Wireless Logic cuenta con el ecosistema de operadores y el portafolio de socios de perfiles eSIM e IMSI más amplio.

Facilidad y costo 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 empresariales y necesidades de despliegue. Navegar el ecosistema RSP por tu cuenta puede ser complejo y costoso, por eso es importante elegir y colaborar con un socio especializado como Wireless Logic.

Conoce más sobre la Aprovisionamiento Remoto de SIM y por qué deberías asociarte con Wireless Logic.

Regresa al Contenido

Autenticación de Dispositivos y Gestión de Identidad

Una identidad de dispositivo única e inmutable es esencial para prevenir la suplantación o el engaño. En otras palabras, para asegurarte de que solo los dispositivos autorizados se comuniquen con tus servidores.

Nosotros resolvemos esto y, además, te permitimos acceder a los dispositivos desde tus servidores mediante una serie de medidas que se describen a continuación.

Solución estándar

Recomendamos el uso de direcciones IP privadas además de la autenticación basada en SIM. Estas medidas, combinadas con APN privado y VPN, ayudan a separar y proteger el tráfico de tus dispositivos del tráfico regular de internet y de las amenazas que pueden existir allí. Si realmente tu industria o tu cliente necesita una dirección IP pública, tenemos soluciones que mejoran la seguridad de esos puntos finales con IP pública.

Opciones de personalización y funciones avanzadas

Usa la SIM para almacenar y distribuir certificados y automatizar la creación y mantenimiento de PKI utilizando nuestra infraestructura segura de IoT SAFE basada en estándares. IoT SAFE es un estándar de GSMA que permite implementar en dispositivos IoT la seguridad basada en certificados que se usa en pagos sin contacto, la industria móvil y de TI.

Los principales beneficios para ti

Una autenticación robusta y una buena gestión de identidades protegen tu red contra suplantación de identidad, ataques de ransomware y accesos no autorizados, que pueden causar pérdida de servicio o tiempos de inactividad en dispositivos o redes.

Facilidad y Coste de adopción

WOfrecemos soluciones de IP privada y APN como estándar. La adopción empresarial de IoT SAFE requiere algo de planificación y colaboración con equipos OEM/ODM y de la nube/servidor, pero por lo demás es muy rentable y puede generar ahorros en la lista de materiales y en el costo total de propiedad de la gestión de identidades (certificados).

Aprende más sobre la seguridad del IoT y por qué deberías asociarte con Wireless Logic.

Red Privada Segura

Más del 95 % de las conexiones IoT gestionadas por Wireless Logic utilizan NetPro, nuestra infraestructura de servicios de APN privado y VPN.

Los servicios de NetPro forman una parte fundamental de tu defensa contra amenazas de seguridad y se combinan con los cifrados del operador y los protocolos de cifrado basados en IP, como TLS, para proporcionar cifrado de extremo a extremo de los datos en tránsito.

Solución estándar

Recomendamos el uso de APNs privados como estándar. Un APN es una puerta de enlace que permite a los dispositivos IoT utilizar la infraestructura de redes móviles para conectarse a redes empresariales sin necesidad de acceder a internet público. Nuestra infraestructura NetPro incluye enlaces de fibra de alta capacidad hacia redes de operadores y se implementa en centros de datos con resiliencia geográfica para maximizar la fiabilidad.

Opciones de personalización y funcionalidades avanzadas

Los VPNs IPSec son típicos para VPNs de sitio a sitio (conectando Wireless Logic con la infraestructura empresarial), y los VPNs SSL se utilizan para accesos remotos puntuales. A menos que ya estés usando cifrado TLS de extremo a extremo en el tráfico entre tu dispositivo y el servidor, los VPNs IPSec son esenciales.

Los principales beneficios para ti

Usa soluciones de red privada segura para prevenir el robo de datos, ransomware, malware y ataques de intermediarios, y así proteger tu marca y reputación.

Facilidad y coste de adopción

Los APNs privados y el cifrado del operador vienen como estándar. Los VPNs requieren cierta planificación entre los equipos de operaciones de red de cada lado, pero deberían usarse en todos los casos, salvo en unos pocos donde solo se transmite la información más simple (encendido/apagado) o datos de sensores. Consulta ***Device Authentication and Identity Management*** para obtener detalles sobre la implementación rentable de TLS en IoT.

Conoce más sobre Secure Private Networking y por qué deberías asociarte con Wireless Logic.

Regresa al Contenido

Funciones centrales de alta disponibilidad e interconexiones

Wireless Logic opera una red central dedicada al IoT, diseñada y construida específicamente para el IoT.

Esto se suma a la infraestructura central y de red de radio de los operadores asociados. En todos los casos, las funciones centrales se ejecutan en infraestructuras de centros de datos geográficamente dispersos, con fuentes de energía independientes para garantizar la fiabilidad y la resiliencia.

Solución estándar

Nuestra infraestructura central opera en un modo activo-activo, lo que garantiza una visión continua del estado de nuestros sistemas y un failover disponible para todo el tráfico en caso de degradación del servicio. El tiempo de restauración del servicio, si un dispositivo necesita establecer una nueva conexión, se gestiona automáticamente redirigiendo el tráfico al nodo activo sin necesidad de intervención manual.

Opciones de personalización y funcionalidades avanzadas

También operamos una red de Packet Gateways distribuidos para proporcionar conexiones de datos localizadas y de baja latencia hacia servicios de red empresarial o de internet.

Recomendamos el uso de direcciones IP duales para los dispositivos, mapeándolas a packet gateways redundantes para automatizar los procesos de failover y recuperación ante interrupciones, en caso de que ocurra alguna.

Los principales beneficios para ti

Nuestras aplicaciones de misión crítica están estructuradas como microservicios y se ejecutan en clústeres de Kubernetes, estratégicamente ubicados en múltiples centros de datos. La configuración activo-activo garantiza alta disponibilidad y confiabilidad, mientras minimiza el riesgo de inactividad.

Facilidad y coste de adopción

El mapeo del tráfico entre los packet gateways centrales y regionales requiere planificación previa, pero la adopción de Conexa es, por lo demás, fluida. Si se utilizan direcciones IP duales, los servidores deben resolver usando DNS antes de contactar con los dispositivos remotos.

Conoce más sobre Conexa y por qué deberías asociarte con Wireless Logic.

Plataforma de gestión de IoT

El monitoreo y la gestión de dispositivos IoT a nivel de conexión, dispositivo, seguridad y aplicación son esenciales para la detección y resolución de incidentes operativos y de seguridad.

Esto incluye la detección de consumo de datos no autorizado, ubicación, estado del dispositivo y anomalías a nivel del sistema o de la aplicación. La detección en tiempo real y las reacciones proactivas serán fundamentales para prevenir pérdidas de servicio generalizadas y caídas del sistema.

Solución estándar

SIMPro es nuestra quinta generación de Plataforma de Gestión de Conectividad, que ha evolucionado para incluir gestión a nivel de Dispositivo (DevicePro), Seguridad (NetPro) y Aplicación (Kheiron). La primera línea de defensa es SIMPro, que supervisa la ubicación, la frecuencia y el volumen de consumo, y puede alertar, limitar, bloquear o poner en cuarentena las conexiones que violen los parámetros que tú definas.

Opciones de personalización y funcionalidades avanzadas

DevicePro te permite supervisar el estado de salud de los dispositivos (intensidad de señal, niveles de batería, temperatura) y realizar configuraciones OTA o actualizaciones de firmware. Kheiron es nuestra plataforma de habilitación de aplicaciones que incluye Gemelo Digital y contextualización y visualización de datos de aplicaciones, con notificaciones push móviles, alertas por SMS y correo electrónico.

Consulta también ***Anomaly & Threat Detection***

Los principales beneficios para ti

Un informe de IBM sobre seguridad de datos de 2022 identificó que el tiempo promedio para detectar y reportar una brecha de seguridad era de aproximadamente 9 meses. La supervisión en tiempo real y a múltiples niveles es crucial para acelerar la detección, tomar medidas correctivas y minimizar los daños causados por incidentes operativos o de ciberseguridad.

Facilidad y coste de adopción

Estos servicios son obligatorios. Las empresas deben aplicar monitoreo a nivel de conectividad, dispositivo, seguridad y aplicación de acuerdo con su perfil de riesgo y tolerancia a la pérdida o corrupción de datos o servicios.

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

Detección de Anomalías y Amenazas (DAA)

Proveedores de soluciones, integradores de sistemas IT/OT y empresas usuarias finales utilizan la Detección de Anomalías y Amenazas para identificar las primeras señales de ciberataques contra sus sistemas IoT.

También les proporciona medidas de gestión de amenazas, visibilidad operativa y respalda sus esfuerzos de cumplimiento con los reguladores de la industria y del gobierno.

Solución Estándar

Los encabezados de paquetes de las comunicaciones entre el dispositivo y la nube se pueden reflejar desde nuestro núcleo móvil hacia nuestro motor de Detección de Anomalías y Amenazas para un análisis impulsado por IA casi en tiempo real, con información y niveles de amenaza comunicados a través de la interfaz de usuario para su investigación y acción correctiva. Estos procesos te alertarán sobre usos anómalos o comunicaciones inusuales de los dispositivos finales y te proporcionarán advertencias sobre malware o eventos de ransomware.

Opciones de personalización y funcionalidades avanzadas

También están disponibles extensiones del servicio para apoyar una integración más estrecha con tus sistemas empresariales y la automatización de respuestas, prevención de amenazas y generación de informes de cumplimiento. Estos informes te proporcionarán evidencia importante de las medidas de monitoreo y prevención que tienes implementadas, información que los reguladores del gobierno buscarán en caso de que experimentes una brecha de seguridad.

Los principales beneficios para ti

Si no se detectan o resuelven, los ciberataques pueden provocar desafíos operativos crónicos, pérdida de reputación y sanciones económicas. La Detección de Anomalías y Amenazas reduce este riesgo y proporciona evidencia crucial de tu estrategia de monitoreo en caso de que necesites demostrarla ante los reguladores.

Facilidad y coste de adopción

La implementación de la Detección de Anomalías y Amenazas es sencilla. No requiere instalar agentes de software en los dispositivos IoT y no compromete el rendimiento de tu sistema ni tus compromisos con la privacidad de los datos.

Conoce más sobre la Detección de Anomalías y Amenazas 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 América del Norte.

SIM Assist es nuestra solución de soporte integral que incluye al asistente digital "Wilo", basado en inteligencia artificial, aprendizaje automático y procesamiento de lenguaje natural, para automatizar solicitudes de servicio rutinarias y liberar a los agentes de soporte para que puedan encargarse de servicios más complejos y centrados en el cliente.

Solución estándar

SIM Assist es un servicio de tres niveles e incluye SIM Assist Enterprise, diseñado para proveedores de soluciones de primer nivel, OEMs y empresas. Ofrece ayuda experta para las soluciones más complejas, incluyendo soporte 24/7 para incidentes P1 y P2.

SIM Assist Enterprise cuenta con los acuerdos de nivel de servicio (SLA) más rápidos para tiempos de primera respuesta en todos los niveles e incluye funciones premium como informes proactivos de incidentes, informes de análisis de causa raíz para incidentes P1 y un agente de atención dedicado.

Los principales beneficios para ti

Una vez que te hayas incorporado como cliente, puedes aprovechar la experiencia de nuestros equipos distribuidos de operaciones de red y servicio alrededor del mundo, quienes te brindan soporte localizado y en tiempo real para tus implementaciones de IoT. El equipo está enfocado en ayudarte a desplegar, escalar y mantener soluciones de alta disponibilidad.

Facilidad y coste de adopción

Nuestros niveles de servicio están diseñados para satisfacer las demandas y presupuestos de implementaciones IoT locales, regionales y globales.

Conoce más sobre las Operaciones Globales 24/7 y por qué deberías asociarte con Wireless Logic.

Casos prácticos

Los Proveedores de Servicios de Conectividad (CSP) desempeñan un papel fundamental al conectar activos, sistemas y personas en ubicaciones remotas. Aunque el propósito principal es conectar el punto A con el punto B, el rol del CSP también abarca la seguridad, la privacidad, la fiabilidad y el cumplimiento de normativas específicas de cada sector.

Esto se ilustra con tres casos de estudio que cubren la telemática de vehículos, la atención sanitaria y los puntos de carga para vehículos eléctricos. Estos casos cruzan los sectores automotriz, energético y de transporte, así como los requisitos relacionados con la privacidad de los datos para clientes comerciales y consumidores. Todo esto se refleja en un amplio conjunto de regulaciones que deben cumplirse.

Regresa al Contenido

Caso práctico 1: **Telemática de Vehículos**

Los dispositivos de telemática vehicular tienen requisitos de movilidad y deben cumplir con las regulaciones automotrices, además de las normas sobre privacidad de datos, seguridad, emisiones de vehículos y las regulaciones operativas que se indican a continuación.

El cumplimiento de numerosas regulaciones depende de servicios de conectividad confiables y ciberresilientes.

Privacidad y Seguridad de los Datos

Los sistemas telemáticos recopilan datos personales y del vehículo, incluyendo el comportamiento del conductor, la ubicación y el rendimiento. El RGPD exige que los gestores de flotas garanticen el procesamiento, almacenamiento y transferencia seguros de estos datos. Los datos personales deben ser anonimizados o encriptados, y el acceso debe estar restringido.

Tributación e Informes

Los datos telemáticos se utilizan para calcular el kilometraje del vehículo, el consumo de combustible y las emisiones con fines de declaración de impuestos.

Seguridad y Mantenimiento del Vehículo

La telemática puede rastrear el mantenimiento del vehículo, el comportamiento del conductor, las inspecciones de seguridad y registrar/reportar incidentes como accidentes o infracciones de seguridad.

Ciberseguridad

ISO/SAE 21434 y NIST CSF proporcionan pautas de ciberseguridad para vehículos de carretera, incluidos los sistemas telemáticos. Los gestores de flotas deben asegurarse de que las soluciones telemáticas cumplan con estas pautas para protegerse contra ciberataques y accesos no autorizados a los datos.

Informe e Investigación de Accidentes

En caso de un accidente, los sistemas telemáticos proporcionan datos detallados sobre el evento, como la velocidad, la ubicación y el comportamiento del conductor, lo cual puede ser crucial para reclamaciones de seguros e investigaciones.

Regulaciones Internacionales para Flotas

Para las flotas que operan en varios países, los sistemas telemáticos deben garantizar el cumplimiento de las normas internacionales de vehículos, como las establecidas por la Unión Internacional de Transporte por Carretera (IRU), y respetar las leyes de privacidad de datos en cada jurisdicción.

Registro, Retención y Acceso a los Datos

En algunas jurisdicciones, los gestores de flotas están obligados a usar dispositivos de registro electrónico para llevar un control de las horas de servicio (HOS) de los conductores. Debes conservar los registros durante al menos seis meses y tenerlos disponibles para que las autoridades los inspeccionen cuando lo soliciten.

Regulaciones Ambientales y de Emisiones

Muchas empresas están obligadas a informar sobre su huella de carbono, y los gestores de flotas deben hacer un seguimiento del consumo de combustible y las emisiones de los vehículos mediante sistemas telemáticos para cumplir con los requisitos de informes de sostenibilidad corporativos o gubernamentales, así como con las normativas de zonas de aire limpio o de emisiones.

Seguros y Gestión de Riesgos

Muchos gestores de flotas usan la telemática para calificar en programas de seguros basados en el uso, donde las primas se calculan según el comportamiento de conducción en tiempo real, el kilometraje y los factores de riesgo. Las aseguradoras suelen requerir datos telemáticos específicos, incluyendo métricas del comportamiento del conductor como el exceso de velocidad, frenadas bruscas y aceleraciones.

Licencias de Conductor y Vehículos

La telemática puede rastrear las calificaciones del conductor o certificaciones médicas y enviar alertas cuando sea necesario renovarlas o actualizarlas. Los administradores de flotas deben asegurarse de que todos los vehículos de la flota estén debidamente registrados, asegurados y cumplan con los requisitos de licencia según su peso, tipo de carga y jurisdicción.

Regresa al Contenido

Caso práctico 2: Puntos de Carga Para Vehículos Eléctricos

La carga de vehículos eléctricos es un mercado altamente competitivo, donde la experiencia del cliente y su lealtad añaden una dimensión adicional a los numerosos estándares legislativos, incluyendo regulaciones de confiabilidad diseñadas para asegurar que los subsidios gubernamentales se usen de manera responsable y que la transición hacia los vehículos eléctricos y la neutralidad de carbono no se vea comprometida.

A continuación se presenta una lista más amplia, aunque no exhaustiva, de regulaciones, incluyendo aquellas que ofrecen protección tanto al consumidor como a la red eléctrica. El cumplimiento de muchas de estas regulaciones se basa en servicios de conectividad confiables y con resiliencia cibernética.

Normas de seguridad eléctrica
Los cargadores de vehículos eléctricos deben cumplir con las normas de seguridad eléctrica como la IEC 61851, UL 2202/2594.

Transparencia de Precios
A menudo, se requiere que los operadores de estaciones de carga muestren claramente los precios por el uso de energía.

Permisos y Zonificación
La instalación de infraestructura de carga normalmente requiere permisos de construcción y debe cumplir con las regulaciones de zonificación.

Integración a la Red
Los operadores de respuesta a la demanda pueden necesitar cumplir con los requisitos de las compañías eléctricas o de los entes reguladores relacionados con los programas de respuesta a la demanda, permitiendo que los cargadores reduzcan la carga durante los períodos de alta demanda.

Privacidad de los Datos del Consumidor
Se debe garantizar la protección de los datos del consumidor, incluyendo la información de facturación, los hábitos de carga y la información personal recopilada a través de aplicaciones o redes de carga.

Ciberseguridad
Dada la naturaleza conectada de las redes de carga de vehículos eléctricos, los fabricantes y operadores deben cumplir con las regulaciones de ciberseguridad (por ejemplo, ISO 27001) para protegerse contra hackeos y accesos no autorizados.

Interoperabilidad y Acceso Abierto
Para asegurarte de que los cargadores de vehículos eléctricos funcionen con una variedad de vehículos y redes, los fabricantes (OEMs) y los operadores de puntos de carga (CPOs) deben cumplir con los protocolos de comunicación de carga, incluyendo ISO 15118 y OCPP (Protocolo Abierto de Puntos de Carga).

Regulaciones Ambientales y Energéticas
En algunas jurisdicciones se requiere eficiencia energética e integración de energías renovables.

Normas de accesibilidad
El equipo de carga debe instalarse a alturas y en lugares que sean fácilmente accesibles para todos los usuarios.

Incentivos Gubernamentales y Cumplimiento
Se espera que los operadores cumplan con los Requisitos de Tiempo de Actividad, los Tiempos de Respuesta de Mantenimiento, la Supervisión en Tiempo Real y las regulaciones de Protección al Consumidor y Transparencia, especialmente cuando han aprovechado incentivos gubernamentales.

Requisitos Legales Clave para la Fiabilidad de los Cargadores de Vehículos Eléctricos

La Ley Bipartidista de Infraestructura (EE. UU.) y el Reglamento de Infraestructura de Combustibles Alternativos de la UE (UE) ofrecen financiación para instalar puntos de carga a lo largo de los principales corredores viales, con el requisito de que los puntos de carga estén disponibles el 98% del tiempo.

Del mismo modo, la Estrategia de Infraestructura para Vehículos Eléctricos del gobierno del Reino Unido estableció objetivos para desarrollar una red de carga sólida para el año 2030 e incluye metas para mejorar la fiabilidad y el tiempo de funcionamiento. Los operadores de puntos de carga que no cumplan con los requisitos resumidos a continuación se enfrentan a sanciones económicas.

1 Requisito del 99% de Disponibilidad
El gobierno del Reino Unido introdujo un estándar mínimo de fiabilidad que exige una disponibilidad del 99% para los cargadores rápidos de vehículos eléctricos (VE) en áreas de servicio de autopistas y otros lugares estratégicos. Este requisito asegura que los cargadores públicos de VE estén operativos y disponibles para los conductores al menos el 99% del tiempo.

2 Acuerdo de Nivel de Servicio (SLA) para el Mantenimiento
Los operadores de redes de carga deben mantener las estaciones de carga con altos estándares de fiabilidad y eficiencia. Esto incluye:

Tiempos de Respuesta para el Mantenimiento:
Si un cargador se reporta como defectuoso, los operadores deben responder rápidamente para solucionar el problema, normalmente en cuestión de horas o días, dependiendo del tipo de cargador.

Monitoreo en Tiempo Real:
Se anima a los operadores a utilizar sistemas de monitoreo en tiempo real para asegurar que los cargadores funcionen correctamente y para abordar fallos de forma proactiva antes de que los clientes los experimenten.

3 Protección al Consumidor y Transparencia
El gobierno del Reino Unido también hace hincapié en la transparencia respecto a la disponibilidad y el rendimiento de los cargadores:

Reporte de Fallos y Actualizaciones de Estado:
Los operadores deben proporcionar datos en tiempo real sobre la disponibilidad de los cargadores a través de aplicaciones móviles o sitios web. Esto te ayuda a planificar tus viajes y evitar cargadores que no funcionen.

Puntos de Contacto Claros para Reportar Fallos:
También existen requisitos legales para que los operadores ofrezcan canales claros donde tú puedas reportar cargadores averiados y recibir actualizaciones sobre las reparaciones.

4 Regulaciones de Carga Inteligente
Bajo las Regulaciones de Puntos de Carga Inteligente para Vehículos Eléctricos, todos los cargadores domésticos y de lugar de trabajo deben ser “inteligentes”, lo que significa que pueden:

- Ajustar los tiempos de carga según la demanda de la red.
- Soportar diagnósticos y mantenimiento a distancia, lo que ayuda a reducir el tiempo fuera de servicio y mejorar la fiabilidad general.

Estas medidas buscan aumentar tu confianza como consumidor, reducir la ansiedad por la autonomía y asegurar que la infraestructura de carga de VE sea confiable mientras el Reino Unido acelera su transición hacia los vehículos eléctricos. La conectividad es esencial.

Regresa al Contenido

Caso práctico 3: **Cuidado de la Salud**

Dispositivos y servicios de salud móvil (mHealth) tienen requisitos de movilidad y deben cumplir con una variedad de regulaciones, así como con requisitos operativos y relacionados con la atención.

Una conectividad robusta y segura es la base del éxito operativo y regulatorio de las soluciones de mHealth, asegurando calidad, cumplimiento y confianza en la prestación de servicios de salud, ya sea que se brinden en casa, en la ambulancia o en entornos hospitalarios.

Cumplimiento de la Privacidad de Datos

Leyes como el GDPR y la HIPAA exigen un manejo seguro de los datos. El tiempo de inactividad conlleva riesgos de filtraciones. Las redes confiables y encriptadas aseguran el cumplimiento al proteger tus datos de pacientes durante la transmisión y el almacenamiento.

Interoperabilidad de Dispositivos

La conectividad inconsistente dificulta la comunicación entre dispositivos en los sistemas de salud móvil (mHealth). Las redes estables e interoperables permiten un intercambio de datos sin interrupciones, siguiendo estándares como HL7, FHIR e ISO 13485.

Ciberseguridad y Gestión de Amenazas

Los ciberataques ponen en riesgo la filtración de datos y la interrupción del servicio. Una conectividad ciberresiliente con protección contra DDoS y marcos de confianza cero asegura operaciones de salud móvil (mHealth) seguras y continuas.

Cumplimiento de la Monitorización Remota de Pacientes (RPM)

Las regulaciones exigen datos continuos de RPM para cumplir con las normas y garantizar la calidad del cuidado. Las redes siempre activas con mecanismos de respaldo evitan interrupciones en la monitorización, protegiendo así los resultados del paciente.

Informes Regulatorios y Auditorías

Los problemas de conectividad interrumpen la presentación oportuna de informes, lo que pone en riesgo el cumplimiento. Las redes confiables aseguran el envío preciso de datos en tiempo real para cumplir con las regulaciones y facilitar auditorías sin contratiempos.

Monitoreo y alertas en tiempo real

El tiempo de inactividad interrumpe el monitoreo crítico de salud, retrasa las alertas y pone en riesgo la seguridad del paciente. Una conectividad confiable y de baja latencia asegura un flujo de datos ininterrumpido para diagnósticos e intervenciones oportunas.

Entrega de Servicios de Telesalud

Las llamadas caídas y el retraso durante las consultas virtuales afectan la calidad de la atención. Una conectividad confiable y de alto ancho de banda asegura servicios de telesalud sin interrupciones y una comunicación efectiva entre tú y tu proveedor.

Escalabilidad para Zonas Desatendidas

Expandir la salud móvil (mHealth) a las zonas rurales enfrenta brechas de conectividad. Las redes de área amplia confiables permiten un acceso escalable y equitativo a la atención médica, incluso en regiones con poca infraestructura.

Continuidad en Emergencias y Cuidados Críticos

La pérdida de conectividad retrasa la atención que salva vidas durante las emergencias. Las redes redundantes y resilientes, junto con la computación en el borde, aseguran el acceso a datos en tiempo real y una atención crítica sin interrupciones.

Integridad y Fiabilidad de los Datos del Paciente

La pérdida o corrupción de datos afecta los diagnósticos y el cumplimiento. Las redes ciberresilientes aseguran una transmisión de datos confiable, preservando la precisión, la integridad y la trazabilidad en todos los sistemas.

Consecuencias del tiempo de inactividad para tus operaciones comerciales y la lealtad de tus clientes

Acabamos de usar dos estudios de caso para destacar el papel fundamental que juega la conectividad resiliente en el cumplimiento normativo, y ahora ampliamos la perspectiva para ilustrar los impactos operativos y comerciales del tiempo de inactividad, que podrían ser causados por fallos prolongados de dispositivos (electromecánicos, ambientales, fallos de software o daños), mantenimiento inadecuado, problemas de conectividad o de infraestructura en la nube.

Las consecuencias del tiempo de inactividad varían según el sector, pero todas son críticas a su manera.

Energía y Servicios Públicos

- Interrupciones del servicio
- Detección tardía de problemas
- Ineficiencias operativas
- Riesgos de cumplimiento

Logística

- Pérdida de visibilidad del envío
- Retrasos en la entrega
- Informes inexactos
- Mayor riesgo de robo o pérdida

Vigilancia Digital

- Eventos de seguridad perdidos
- Brechas de datos
- Riesgos de seguridad aumentados
- Incumplimientos de normativa

Carga de vehículos eléctricos

- Ingresos perdidos
- Dificulta la adopción de vehículos eléctricos
- Interrupciones operativas
- Fallos de cumplimiento

Salud

- Atención al paciente retrasada
- Riesgos para la seguridad del paciente
- Daño a la reputación
- Incumplimientos de cumplimiento

Digitalización del personal

- Pérdida de productividad
- Plazos incumplidos
- Fallos en la comunicación
- Riesgos de seguridad/protección

Venta al por menor

- Fallos en transacciones
- Inexactitud en el inventario
- Insatisfacción del cliente
- Retrasos en la cadena de suministro

Telemática de Vehículos

- Pérdida del seguimiento en tiempo real
- Informes de datos inexactos
- Ineficiencias operativas
- Problemas de cumplimiento

Drones y Vehículos Autónomos

- Fallos de navegación
- Peligros para la seguridad
- Interrupciones de la misión
- Respuesta y decisiones retrasadas

Regresa al Contenido

Contacto **Wireless Logic**

La conectividad confiable y la seguridad robusta son fundamentales para mantener la eficiencia operativa, la productividad, la seguridad y la protección en empresas de todos los sectores.

Las regulaciones gubernamentales e industriales exigen un mayor uso de dispositivos conectados y también son cada vez más estrictas en cuanto al tiempo de actividad, la ciberresiliencia y la privacidad de los datos.

Este documento demuestra el papel clave de los Proveedores de Servicios de Comunicación para ayudarte a cumplir con esos requisitos y alcanzar los resultados comerciales que deseas con IoT.

No esperes hasta el día del despliegue para pensar en la conectividad; plánificala desde el principio y cuenta con Wireless Logic como tu socio estratégico en 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 las empresas que usan IoT.

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

Gracias por conectar con Wireless Logic.

Contáctanos

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

Other office locations

Austria
China
Denmark
France
Germany
Italy
Netherlands
Norway
Spain
USA

wirelesslogic.es