Informe Analítico: La Convergencia Estratégica de Cloud Computing e IoT en el Horizonte 2025-2030

Parte I: Computación en la Nube – La Infraestructura Fundamental de la Era Digital

1.1. El Paradigma de la Nube: Marco Conceptual y Características Esenciales

La computación en la nube, o *Cloud Computing*, ha trascendido su estatus de tecnología emergente para consolidarse como el pilar fundamental sobre el que se erige la infraestructura digital contemporánea. Su definición, estandarizada por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST), la describe como un modelo que permite el acceso de red ubicuo, conveniente y bajo demanda a un conjunto compartido de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios.[1] Este modelo no es simplemente una evolución tecnológica, sino un cambio de paradigma en la forma en que las organizaciones y los individuos consumen y gestionan la tecnología de la información.

Para comprender la magnitud de esta transformación, es imperativo deconstruir las cinco características esenciales que, según el NIST, definen intrínsecamente a un servicio de nube [1]:

1. **Autoservicio bajo demanda (On-demand self-service):** Esta característica empodera al usuario final, permitiéndole aprovisionar unilateralmente capacidades de computación, como tiempo de servidor o almacenamiento en red, según sea necesario y de forma automática, sin requerir intervención humana por parte del proveedor de servicios. En la práctica, esto se traduce en una agilidad sin precedentes; un equipo de desarrollo puede

lanzar un nuevo servidor virtual en cuestión de segundos a través de una consola web o una API, en lugar de esperar semanas o meses en un ciclo de adquisición de hardware tradicional.[1]

2. **Acceso amplio a la red (Broad network access):** Las capacidades están disponibles a través de la red y se accede a ellas mediante mecanismos estándar que promueven el uso por parte de plataformas de cliente heterogéneas, tanto ligeras como pesadas (por ejemplo, teléfonos móviles, tabletas, portátiles y estaciones de trabajo).[1] Esta ubicuidad es la que ha permitido el auge del trabajo remoto, la colaboración global en tiempo real y la entrega de servicios a escala planetaria.[2]
3. **Agrupamiento de recursos (Resource pooling):** Los recursos de computación del proveedor se agrupan para servir a múltiples consumidores utilizando un modelo multi-inquilino (*multi-tenant*), con diferentes recursos físicos y virtuales asignados y reasignados dinámicamente según la demanda del consumidor. Existe un sentido de independencia de la ubicación, ya que el cliente generalmente no tiene control ni conocimiento sobre la ubicación exacta de los recursos proporcionados, aunque puede ser capaz de especificar la ubicación a un nivel más alto de abstracción (por ejemplo, país, estado o centro de datos).[1] Esta abstracción y eficiencia a escala es lo que genera las economías que hacen que la nube sea rentable.[5]
4. **Elasticidad rápida (Rapid elasticity):** Las capacidades pueden ser aprovisionadas y liberadas elásticamente, en algunos casos de forma automática, para escalar rápidamente hacia afuera y hacia adentro de acuerdo con la demanda. Para el consumidor, las capacidades disponibles para el aprovisionamiento a menudo parecen ser ilimitadas y pueden ser adquiridas en cualquier cantidad y en cualquier momento.[1] Un ejemplo paradigmático es el escalado automático de una plataforma de comercio electrónico durante un evento de ventas masivas, donde la infraestructura se expande para manejar picos de tráfico y se contrae una vez que la demanda disminuye, optimizando tanto el rendimiento como los costos.[2]
5. **Servicio medido (Measured service):** Los sistemas en la nube controlan y optimizan automáticamente el uso de los recursos aprovechando una capacidad de medición en algún nivel de abstracción apropiado para el tipo de servicio (por ejemplo, almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas). El uso de los recursos puede ser monitoreado, controlado y reportado, proporcionando transparencia tanto para el proveedor como para el consumidor del servicio utilizado.[1]

Si bien esta última característica, "Servicio medido", fue concebida como una capacidad técnica fundamental, su evolución en el mercado maduro de 2025 ha revelado una complejidad estratégica mucho mayor. La capacidad de medir el consumo al detalle ha dado lugar a lo que hoy es el principal desafío para la mayoría de las organizaciones que operan en la nube: la gestión del gasto. Según análisis recientes, el 82% de los responsables de la toma de decisiones en la nube citan la gestión de los costos como su principal preocupación.[7] La facilidad de aprovisionamiento y la complejidad de los modelos de precios de los proveedores a menudo conducen a un gasto descontrolado y a un desperdicio significativo, estimado en

más del 32% de los presupuestos de la nube.[8] Esto ha catalizado el surgimiento de una disciplina empresarial completamente nueva conocida como FinOps (Cloud Financial Operations), cuyo objetivo es inculcar la responsabilidad financiera en el modelo de gasto variable de la nube. Por lo tanto, lo que comenzó como una simple característica de medición se ha transformado en un imperativo de gobernanza financiera, demostrando la maduración del mercado desde la mera provisión técnica hacia la optimización estratégica y económica.

1.2. Jerarquía de Servicios en la Nube: Modelos de Entrega IaaS, PaaS y SaaS

El modelo de computación en la nube se materializa a través de tres modelos de servicio principales, a menudo visualizados como una pila jerárquica: Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS). Cada capa de esta jerarquía representa un nivel diferente de abstracción y gestión, determinando la división de responsabilidades entre el proveedor de la nube y el cliente consumidor del servicio.[1]

Infraestructura como Servicio (IaaS)

IaaS constituye la capa fundamental de la pila de servicios en la nube. En este modelo, el proveedor ofrece acceso a recursos informáticos esenciales, como capacidad de procesamiento (CPU/GPU), memoria (RAM), almacenamiento (en bloque, de archivos y de objetos) y redes.[1] El cliente no gestiona ni controla la infraestructura física subyacente de la nube, pero tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones desplegadas, y un control limitado de componentes de red seleccionados (por ejemplo, firewalls de host).[1] Esencialmente, IaaS proporciona los "bloques de construcción" virtuales para que los usuarios construyan su propia infraestructura de TI en la nube.

El mercado de IaaS está dominado por un oligopolio de proveedores a hiperescala. A mediados de 2025, Amazon Web Services (AWS) mantiene su liderazgo histórico, seguido por Microsoft Azure y Google Cloud Platform (GCP). Estos tres gigantes controlan colectivamente una porción abrumadora del mercado global.[8] Además de estos líderes, existen proveedores de nicho como DigitalOcean y Linode (ahora parte de Akamai) que se diferencian por ofrecer una experiencia de usuario simplificada y precios predecibles, dirigidos principalmente a desarrolladores y pequeñas y medianas empresas.[1]

Tabla 1: Panorama Competitivo de Proveedores de Infraestructura como Servicio (IaaS)

– 2025

Proveedor	Cuota de Mercado (Q2 2025 est.)	Fortalezas Clave	Ecosistema y Servicios Distintivos	Consideraciones/Desafíos
Amazon Web Services (AWS)	31% - 32% [9]	Madurez, amplitud y profundidad del portafolio de servicios (+200), alcance global, ecosistema de socios robusto.	AWS Lambda (Serverless), S3 (Almacenamiento de objetos), EC2 (Cómputo), amplia gama de bases de datos y servicios de IA/ML.	Complejidad de precios, curva de aprendizaje pronunciada debido a la vasta cantidad de servicios.
Microsoft Azure	20% - 23% [8]	Fuerte integración con el ecosistema empresarial de Microsoft (Office 365, Windows Server, Active Directory), capacidades híbridas líderes (Azure Arc).	Azure Synapse Analytics, Power Platform, excelente soporte para cargas de trabajo de Windows y.NET, fuerte enfoque en cumplimiento y seguridad empresarial.	La curva de aprendizaje puede ser más pronunciada para equipos no familiarizados con las tecnologías de Microsoft.
Google Cloud Platform (GCP)	11% - 13% [8]	Liderazgo en Kubernetes (GKE), análisis de datos y Big Data (BigQuery),	Enfoque en la innovación de código abierto, cultura de ingeniería (SRE), precios	Ecosistema de socios y alcance de ventas empresariales aún en

		Machine Learning (Vertex AI), red global de alto rendimiento.	competitivos y amigables para el cliente.	desarrollo en comparación con AWS y Azure.

Plataforma como Servicio (PaaS)

PaaS se sitúa en la capa intermedia, proporcionando a los clientes un entorno completo de desarrollo, despliegue y gestión de aplicaciones sin la complejidad de construir y mantener la infraestructura subyacente asociada.[1] El proveedor gestiona los servidores, el almacenamiento, las redes y los sistemas operativos, mientras que el cliente se centra en el desarrollo y la gestión de sus aplicaciones y datos. PaaS incluye típicamente sistemas operativos, lenguajes de programación, bases de datos y servidores web.[1] Ejemplos notables de proveedores de PaaS incluyen Heroku, Google App Engine y Red Hat OpenShift.[12]

Software como Servicio (SaaS)

SaaS es el modelo más conocido y utilizado por el público general y las empresas. En este modelo, el proveedor ofrece aplicaciones completas a través de la red, generalmente accesibles a través de un navegador web o una interfaz de programa.[1] El cliente no gestiona ni controla ningún aspecto de la infraestructura de la nube, incluyendo red, servidores, sistemas operativos, almacenamiento o incluso las capacidades de la aplicación individual, con la posible excepción de configuraciones de usuario específicas.[1] Ejemplos omnipresentes de SaaS incluyen herramientas de CRM como Oracle Sales Cloud o Salesforce, suites de ofimática como Google Docs y Microsoft 365, y plataformas de streaming como Spotify y YouTube.[1] En términos de ingresos, SaaS representa el segmento más grande del mercado de la nube, impulsado por su facilidad de adopción y su modelo de suscripción predecible.[14]

Es crucial señalar que la distinción tripartita de IaaS, PaaS y SaaS, aunque conceptualmente útil, se ha vuelto cada vez más difusa en el panorama actual. Los principales proveedores de IaaS, como AWS y Azure, han expandido masivamente sus carteras para incluir servicios PaaS robustos, como AWS Elastic Beanstalk o las funciones de Azure App Service.[11] Esta convergencia ha dado paso a un nivel de abstracción aún mayor: la computación sin servidor (*Serverless*). Modelos como AWS Lambda y Google Cloud Run permiten a los desarrolladores ejecutar código en respuesta a eventos sin aprovisionar ni gestionar servidores en absoluto.[2]

Este paradigma *serverless* no encaja nítidamente en la clasificación tradicional, pero representa la máxima expresión de la promesa de la nube: abstraer por completo la infraestructura para que los equipos puedan centrarse exclusivamente en la lógica de negocio y la entrega de valor.

1.3. La Tecnología Habilitadora: Virtualización e Hipervisores

La magia de la computación en la nube, que permite la agrupación de recursos y la elasticidad rápida, es posible gracias a una tecnología fundamental: la virtualización. La virtualización es el proceso de crear una representación basada en software (virtual) de algo, en lugar de una física. En el contexto de la nube, implica simular una o más computadoras completas, conocidas como máquinas virtuales (VMs), dentro de un único servidor físico.[1] Esto se logra mediante la creación de una "capa de abstracción" sobre el hardware, que permite que los componentes físicos de un solo servidor (procesador, memoria, almacenamiento) se dividan en múltiples máquinas virtuales independientes y aisladas entre sí.[1]

La pieza de software que crea y gestiona estas máquinas virtuales se denomina hipervisor. Existen dos tipos principales de hipervisores, pero el que domina el entorno de los centros de datos en la nube es el Hipervisor de Tipo 1, también conocido como "bare-metal".[17] Este tipo de hipervisor se instala y se ejecuta directamente sobre el hardware del servidor anfitrión, actuando como un sistema operativo ligero y altamente optimizado cuya única función es gestionar las VMs. Esta arquitectura proporciona un rendimiento y una eficiencia superiores al tener acceso directo a los recursos físicos del sistema.

El mercado de hipervisores de Tipo 1 está liderado por tres tecnologías clave [17]:

- **VMware vSphere/ESXi:** Considerado durante mucho tiempo el estándar de oro en la virtualización empresarial, es conocido por su robustez, su amplio conjunto de características de gestión avanzada (como vMotion para la migración en vivo de VMs) y su vasto ecosistema.[18]
- **Microsoft Hyper-V:** Es la solución de virtualización de Microsoft, integrada de forma nativa en Windows Server y también disponible en versiones de cliente de Windows. Su principal ventaja es su profunda integración con el ecosistema de Microsoft, lo que lo convierte en una opción natural para organizaciones que ya dependen en gran medida de las tecnologías de Microsoft.[18]
- **KVM (Kernel-based Virtual Machine):** Es una solución de virtualización de código abierto integrada en el kernel de Linux. KVM ha ganado una tracción masiva y sirve como la base tecnológica para muchas de las nubes públicas y privadas más grandes del mundo, así como para plataformas de virtualización populares como Proxmox VE, oVirt y

OpenStack.[17]

Sin embargo, centrarse únicamente en la virtualización de máquinas virtuales sería pasar por alto una de las transformaciones más significativas en la infraestructura de TI de la última década: el auge de la **contenedorización**. Tecnologías como Docker y orquestadores como Kubernetes han introducido una forma de virtualización a nivel de sistema operativo. A diferencia de las VMs, que virtualizan una máquina de hardware completa (incluido su propio kernel de sistema operativo), los contenedores comparten el kernel del sistema operativo del host y solo empaquetan la aplicación y sus dependencias.[4] Esto los hace extremadamente ligeros, portátiles y rápidos de iniciar, con una sobrecarga de recursos mucho menor que las VMs.

La contenedorización no ha reemplazado a la virtualización de VMs, sino que la complementa. Las VMs proporcionan un fuerte aislamiento a nivel de hardware, mientras que los contenedores ofrecen agilidad y eficiencia para desplegar aplicaciones, especialmente aquellas basadas en arquitecturas de microservicios. Hoy en día, los principales proveedores de la nube ofrecen servicios de orquestación de contenedores gestionados (como Amazon EKS, Azure AKS y Google GKE) que son tan estratégicos y fundamentales para sus plataformas como sus servicios de máquinas virtuales. Por lo tanto, el panorama de la virtualización en 2025 es un ecosistema dual, donde las VMs y los contenedores coexisten para satisfacer diferentes necesidades de las cargas de trabajo modernas, un matiz crucial que no estaba presente en las discusiones iniciales sobre la tecnología de la nube.

1.4. Implicaciones Estratégicas: Un Balance de Ventajas y Desafíos

La adopción de la computación en la nube ofrece un conjunto convincente de ventajas estratégicas que han impulsado su adopción masiva en todas las industrias. Sin embargo, también presenta un nuevo conjunto de desafíos que las organizaciones deben gestionar cuidadosamente para materializar plenamente su valor.

Ventajas Estratégicas:

- **Reducción de Costos e Inversiones (CAPEX a OPEX):** La nube transforma el gasto en infraestructura de un modelo de inversión de capital (CAPEX) a un modelo de gasto operativo (OPEX). En lugar de realizar grandes inversiones iniciales en hardware y centros de datos, las empresas pagan solo por los recursos que consumen, lo que reduce las barreras de entrada y libera capital para otras iniciativas estratégicas.[1]
- **Agilidad y Velocidad de Comercialización:** La capacidad de aprovisionar recursos en minutos permite a los equipos de desarrollo y operaciones experimentar, iterar y lanzar nuevos productos y servicios a un ritmo antes inimaginable. Esta agilidad es una ventaja

competitiva crítica en los mercados dinámicos de hoy.[2]

- **Flexibilidad y Escalabilidad:** La nube ofrece una elasticidad casi infinita, permitiendo a las empresas escalar sus operaciones globalmente para satisfacer la demanda de los clientes sin preocuparse por las limitaciones de la infraestructura física. Esta capacidad de escalar hacia arriba o hacia abajo según sea necesario garantiza un rendimiento óptimo y una eficiencia de costos.[1]
- **Accesibilidad y Colaboración Global:** Al estar basados en la red, los servicios en la nube son accesibles desde cualquier lugar con una conexión a Internet, lo que facilita el trabajo remoto, la colaboración entre equipos distribuidos geográficamente y la prestación de servicios a una base de clientes global.[1]

Desafíos Contemporáneos:

- **Dependencia del Proveedor (*Vendor Lock-in*):** A medida que las organizaciones integran más profundamente sus operaciones con los servicios específicos y propietarios de un proveedor de la nube, la migración a otro proveedor puede volverse técnica y económicamente prohibitiva. Esta dependencia es una preocupación estratégica significativa.[1]
- **Complejidad de la Gestión de Costos:** Como se mencionó anteriormente, la facilidad de uso de la nube puede llevar a un gasto descontrolado. La gestión eficaz de los costos en entornos de nube complejos, a menudo multicloud, se ha convertido en el principal desafío operativo, requiriendo nuevas herramientas y habilidades (FinOps).[7]
- **Gobernanza y Cumplimiento:** Operar en la nube requiere marcos de gobernanza sólidos para gestionar el acceso, los datos y el cumplimiento de regulaciones como GDPR o HIPAA, especialmente en entornos multiregionales y multicloud.[7]
- **Seguridad y Responsabilidad Compartida:** La seguridad en la nube presenta una aparente paradoja. Inicialmente percibida como una desventaja ("la seguridad está en manos de un tercero") [1], la realidad es más matizada. La investigación actual muestra que el 94% de las empresas informan de *mejoras* en su postura de seguridad después de migrar a la nube.[7] Esto se debe a que los proveedores a hiperescala invierten miles de millones en seguridad y emplean a los mejores expertos del mundo, ofreciendo una infraestructura subyacente mucho más segura de lo que la mayoría de las organizaciones podrían construir por sí mismas.[2]

La paradoja se resuelve al comprender el **modelo de responsabilidad compartida**. El proveedor es responsable de la seguridad *de* la nube (la infraestructura física, la red, el hipervisor), mientras que el cliente es responsable de la seguridad *en* la nube (la configuración de los servicios, la gestión de identidades y accesos, la protección de los datos). La gran mayoría de las brechas de seguridad en la nube no se deben a una falla del proveedor, sino a una mala configuración por parte del cliente, que representa hasta el 68% de los incidentes.[7] Por lo tanto, la seguridad en la nube no es inherentemente un riesgo mayor, sino un tipo de riesgo diferente. El desafío se traslada de la gestión de la seguridad física a la gestión rigurosa de la configuración, las identidades y los permisos, lo que exige un nuevo

conjunto de habilidades, herramientas de automatización y un enfoque de gobernanza de la seguridad en la nube.

Parte II: Internet de las Cosas (IoT) – La Digitalización del Mundo Físico

2.1. El Ecosistema IoT: Definición, Arquitectura y Ciclo de Vida de los Datos

El Internet de las Cosas (IoT, por sus siglas en inglés) representa la siguiente fase en la evolución de Internet, extendiendo la conectividad más allá de las computadoras y los teléfonos inteligentes para abarcar un vasto universo de objetos físicos cotidianos. Se define como un conjunto de tecnologías y protocolos asociados que permiten que los objetos se conecten a una red de comunicaciones, sean identificados y controlados a través de esta conexión.[1] La Unión Internacional de Telecomunicaciones (UIT) lo define de manera más formal como una "infraestructura global para la sociedad de la información, que permite servicios avanzados mediante la interconexión de cosas (físicas y virtuales) basadas en tecnologías de la información y la comunicación interoperables existentes y en evolución".[1] En esencia, IoT es el tejido conectivo que digitaliza el mundo físico, permitiendo la interacción entre máquinas y personas (P2M) y, de manera crucial, entre máquinas y máquinas (M2M).[1]

La **arquitectura general** de un sistema IoT, aunque puede variar en complejidad, sigue un patrón de capas bien definido [1]:

1. **Capa de Percepción (Things):** Es la capa física, compuesta por los "objetos" o "cosas". Estos objetos están equipados con sensores para recopilar datos de su entorno (temperatura, movimiento, luz, etc.) y/o actuadores para realizar acciones en el mundo físico (abrir una cerradura, ajustar un termostato, etc.). Tecnologías como las etiquetas de Identificación por Radiofrecuencia (RFID) son fundamentales en esta capa para la identificación única de objetos.[1]
2. **Capa de Red (Connectivity):** Esta capa es responsable de transmitir los datos recopilados por los sensores a un sistema de procesamiento central. Incluye una variedad de tecnologías de comunicación, desde redes de área personal de corto alcance como Bluetooth y ZigBee, hasta redes de área local como Wi-Fi, y redes de área amplia como las redes celulares (4G, 5G, y variantes de bajo consumo como NB-IoT y 5G

RedCap).[1]

3. **Capa de Procesamiento (Gateway & Cloud):** Los datos brutos de los sensores a menudo se envían a una puerta de enlace (*gateway*) local para un pre-procesamiento o agregación antes de ser transmitidos a la nube. La nube (o un centro de datos de back-end) actúa como el cerebro del sistema, proporcionando la capacidad de almacenamiento masivo y la potencia de cómputo necesaria para procesar, analizar y almacenar los datos de IoT.[1]
4. **Capa de Aplicación (Business Data Analysis):** En esta capa superior, los datos procesados se transforman en información útil y se presentan a los usuarios finales a través de aplicaciones, paneles de control o se utilizan para activar alertas y acciones automatizadas. Es aquí donde se genera el valor de negocio, utilizando análisis de datos, inteligencia artificial y aprendizaje automático para obtener conocimientos y optimizar procesos.[1]

Este flujo de datos a través de la arquitectura se puede conceptualizar como el **Ciclo de Vida de los Datos de IoT** [1]:

- **Ocurrencia:** Una actividad o un estado en el mundo físico es detectado por un sensor en un objeto.
- **Recolección:** Los datos brutos del sensor se transmiten desde el objeto a través de una red de comunicaciones.
- **Agregación:** Los datos de múltiples sensores y fuentes se agrupan, se clasifican y se estructuran para convertirse en información coherente.
- **Almacenamiento:** La información agregada se almacena en bases de datos, generalmente en la nube, para su posterior análisis.
- **Interpretación:** La información almacenada se analiza utilizando herramientas de software (a menudo con IA/ML) para extraer conocimientos, identificar patrones o tomar decisiones. Este conocimiento se presenta a los usuarios o se utiliza para mejorar los procesos de negocio.
- **Acción:** Basado en la interpretación, se envían comandos a los actuadores en el mundo físico para realizar una acción, completando así el ciclo de retroalimentación.

Este ciclo ilustra cómo IoT crea un puente bidireccional entre el mundo físico y el digital, permitiendo no solo monitorear, sino también controlar y optimizar activamente el entorno físico a una escala sin precedentes.

2.2. Aplicaciones Transformadoras del IoT

El potencial de IoT no es teórico; ya está transformando una amplia gama de industrias y aspectos de la vida cotidiana. Su capacidad para recopilar datos del mundo real en tiempo

real y actuar sobre ellos abre un abanico de aplicaciones que mejoran la eficiencia, la seguridad y la calidad de vida.[1]

- **Industria 4.0 y Fábricas Inteligentes (Smart Factory):** En el sector manufacturero, IoT es la piedra angular de la Cuarta Revolución Industrial. Los sensores en la maquinaria de producción monitorean continuamente su estado de salud, permitiendo el **mantenimiento predictivo**, que anticipa fallos antes de que ocurran, reduciendo drásticamente el tiempo de inactividad no planificado.[25] Las cadenas de suministro se vuelven transparentes y eficientes mediante el seguimiento de activos en tiempo real, desde el almacén hasta la entrega final. Además, los dispositivos *wearables* y las cámaras de visión por computadora mejoran la seguridad de los trabajadores al detectar condiciones peligrosas o fatiga.[1]
- **Ciudades Inteligentes (Smart Cities):** Los gobiernos y municipios utilizan IoT para abordar desafíos urbanos complejos. Las aplicaciones incluyen la **gestión inteligente del tráfico** mediante sensores que ajustan los semáforos en tiempo real para optimizar el flujo de vehículos, la **iluminación pública inteligente** que reduce el consumo de energía al atenuar las luces cuando no hay nadie cerca, y el **monitoreo ambiental** que mide la calidad del aire y los niveles de ruido para informar políticas de salud pública.[1] La gestión de infraestructuras críticas, como puentes y tuberías de agua, también se beneficia del monitoreo de IoT para detectar necesidades de mantenimiento antes de que se produzcan fallos catastróficos.[25]
- **Salud Conectada (Connected Health):** En el ámbito de la salud, IoT está revolucionando tanto la atención hospitalaria como el monitoreo remoto de pacientes. Los dispositivos *wearables* como pulseras inteligentes y relojes monitorean los signos vitales de los pacientes en sus hogares, permitiendo a los médicos intervenir proactivamente.[1] Dentro de los hospitales, los equipos médicos conectados rastrean su ubicación y estado de uso, optimizando la utilización de activos. Un ejemplo paradigmático, aunque también una advertencia sobre la seguridad, es el marcapasos con conectividad Wi-Fi, que puede ser monitoreado y ajustado remotamente por un cardiólogo, pero que también introduce nuevas superficies de ataque si no se asegura adecuadamente.[1]
- **Hogar Inteligente (Smart Home):** En el ámbito del consumidor, los dispositivos de IoT han proliferado, desde termostatos que aprenden las preferencias de los usuarios para optimizar la calefacción y el aire acondicionado, hasta sistemas de seguridad que permiten a los propietarios monitorear sus hogares de forma remota. La automatización de tareas cotidianas, como encender las luces o preparar el café, mejora la comodidad y la eficiencia energética.[1]
- **Transporte y Logística:** Este sector fue uno de los primeros en adoptar tecnologías M2M. La gestión de flotas utiliza IoT para rastrear la ubicación de los vehículos, monitorear el comportamiento del conductor y optimizar las rutas para ahorrar combustible. En la logística, el seguimiento de paquetes en tiempo real y el monitoreo de las condiciones de los contenedores (por ejemplo, la temperatura para productos

perecederos) garantizan la integridad de la cadena de suministro.[1]

Estas aplicaciones demuestran que el valor de IoT no reside en la mera conexión de objetos, sino en la capacidad de transformar los datos generados por estos objetos en conocimientos procesables, automatización inteligente y, en última instancia, en una mayor eficiencia y mejores resultados de negocio. Según estudios, las empresas que utilizan extensivamente tecnologías IoT pueden llegar a ser un 10% más rentables debido a estas ganancias de eficiencia.[1]

2.3. Desafíos Críticos del Ecosistema IoT

A pesar de su inmenso potencial transformador, la expansión exponencial del Internet de las Cosas ha traído consigo un conjunto de desafíos críticos que deben ser abordados para garantizar un desarrollo seguro, sostenible y confiable. Estos desafíos abarcan la seguridad, la gobernanza de datos, la privacidad y la interoperabilidad.[1]

Seguridad: El Talón de Aquiles del IoT

La seguridad es, con diferencia, el desafío más apremiante y complejo del ecosistema IoT. Cada dispositivo conectado representa un nuevo punto de entrada potencial a una red, y la superficie de ataque se expande con cada nuevo sensor o actuador desplegado. Las predicciones de 2015, que advertían que el 90% de las redes de TI enfrentarían problemas de seguridad originados en IoT, se han materializado de forma dramática.[1] De hecho, los ataques de malware dirigidos específicamente a dispositivos IoT experimentaron un crecimiento del 400% en un solo año, siendo el sector manufacturero el más afectado.[24]

La vulnerabilidad inherente de muchos dispositivos IoT se debe a una combinación de factores:

- **Firmware Inseguro:** Muchos dispositivos se fabrican con un enfoque en el bajo costo y la rápida comercialización, a menudo a expensas de la seguridad. El firmware puede contener vulnerabilidades conocidas que no son parcheadas o, en algunos casos, no pueden ser parcheadas.[28]
- **Credenciales por Defecto:** Una de las prácticas más peligrosas es el uso de nombres de usuario y contraseñas de administrador por defecto, que a menudo son débiles (ej. "admin"/"password") y comunes a miles de dispositivos. Los atacantes explotan estas credenciales para crear masivas *botnets* de IoT, como la infame Mirai.[22]

- **Falta de Cifrado:** Muchas comunicaciones entre dispositivos IoT y sus servidores en la nube no están cifradas por defecto, lo que las hace susceptibles a ataques de intermediario (*Man-in-the-Middle*), donde un atacante puede interceptar, leer y manipular los datos en tránsito.[28]

La comprensión de la seguridad en IoT ha evolucionado significativamente. Los enfoques iniciales se centraban en la seguridad del dispositivo individual. Sin embargo, la experiencia ha demostrado que asegurar el IoT requiere una estrategia de ecosistema holística, una arquitectura de defensa en profundidad que abarque el dispositivo, la red, la nube y las APIs. Las estrategias de mitigación modernas van mucho más allá de las prácticas básicas y se centran en principios arquitectónicos avanzados.

Tabla 2: Matriz Evolutiva de Riesgos de Seguridad en IoT y Estrategias de Mitigación Modernas

Dominio de Riesgo (Identificado en 2015)	**Manifestación de la Amenaza (Ejemplos Actuales)**	**Estrategia de Mitigación Primaria (Concepto Moderno)**	**Tecnologías y Prácticas Específicas**
Suplantación de identidad de dispositivos	Dispositivos falsificados o comprometidos inyectan datos maliciosos o reciben comandos no autorizados. Ataques a infraestructuras críticas.	**Identidad de Dispositivo Fuerte (Zero Trust)**	Infraestructura de Clave Pública (PKI) para emitir certificados digitales únicos (x.509) a cada dispositivo, garantizando una autenticación mutua y segura. Aprovisionamiento seguro de identidades en la fabricación.[30]
Datos comprometidos en tránsito	Ataques *Man-in-the-Middle* (MitM) para espiar comunicaciones (ej. datos de	**Cifrado de Extremo a Extremo**	Uso de protocolos de comunicación seguros como TLS 1.3 para TCP y DTLS para UDP. Cifrado

	pacientes de un monitor de salud) o alterar datos (ej. cambiar lecturas de sensores industriales).		de los datos desde el sensor hasta la aplicación final en la nube, impidiendo que intermediarios (incluido el proveedor de red) puedan leerlos.[28]
Control no autorizado de dispositivos / Interrupción del servicio	Creación de *botnets* de IoT (ej. Mirai) utilizando dispositivos vulnerables para lanzar ataques de Denegación de Servicio Distribuido (DDoS) a gran escala.	**Segmentación de Red y Control de Acceso de Mínimo Privilegio**	Aislar los dispositivos IoT en segmentos de red separados (VLANs o microsegmentación) para que un dispositivo comprometido no pueda afectar a la red corporativa crítica. Implementar firewalls y políticas de control de acceso basado en roles (RBAC).[22]
Software/Firmware comprometido	Explotación de vulnerabilidades conocidas en el firmware para tomar el control total del dispositivo. Inyección de malware a través de mecanismos de actualización inseguros.	**Ciclo de Vida de Desarrollo Seguro y Actualizaciones Seguras (OTA)**	Implementar un proceso de "seguridad por diseño" desde el inicio. Utilizar mecanismos de actualización por aire (OTA) que validen criptográficamente la integridad y autenticidad del firmware antes de la instalación. Mantener un

			inventario de dispositivos y aplicar parches de forma oportuna.[30]
Análisis de datos interrumpido / Servidores hackeados	Ataques a las plataformas en la nube que gestionan los dispositivos IoT, comprometiendo los datos de millones de dispositivos a la vez. Explotación de APIs inseguras.	**Seguridad en la Nube y de APIs**	Aplicar las mejores prácticas de seguridad en la nube (gestión de identidades y accesos, cifrado en reposo). Proteger las APIs con autenticación robusta (ej. OAuth 2.0), autorización y limitación de velocidad para prevenir abusos.[28]

Gobernanza de Datos y Privacidad

El IoT genera cantidades masivas de datos, a menudo de naturaleza personal y sensible. Esto plantea profundos dilemas sobre la privacidad, el consentimiento y la propiedad de los datos, encapsulados en la pregunta: "¿cuánto y cuándo quiero ser monitoreado?".[1] Las organizaciones que despliegan soluciones de IoT deben navegar por un complejo panorama de regulaciones de protección de datos, como el Reglamento General de Protección de Datos (GDPR) en Europa o la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) en Estados Unidos, que imponen requisitos estrictos sobre cómo se recopilan, procesan y almacenan los datos personales.[30]

Interoperabilidad y Estandarización

Para que el IoT alcance su máximo potencial, los dispositivos de diferentes fabricantes deben poder comunicarse entre sí de manera fluida. Históricamente, la falta de estándares universales ha llevado a la creación de ecosistemas cerrados y fragmentados. Aunque se han

realizado esfuerzos de estandarización por parte de organismos como la UIT, el IETF y alianzas como ZigBee [1], el desafío persiste. Sin embargo, están surgiendo estándares más nuevos y prometedores. En el ámbito del hogar inteligente, el protocolo Matter, respaldado por los principales gigantes tecnológicos, busca crear una capa de aplicación unificada. En el ámbito de la conectividad celular, tecnologías como 5G RedCap (Reduced Capability) están siendo diseñadas específicamente para casos de uso de IoT, ofreciendo un equilibrio entre rendimiento y eficiencia energética.[23] La adopción de estos estándares será crucial para fomentar un ecosistema de IoT verdaderamente abierto e interoperable.

Parte III: Síntesis y Prospectiva Estratégica (2025-2030)

3.1. La Relación Simbiótica: Por Qué la Nube es Indispensable para el IoT

La relación entre el Internet de las Cosas y la Computación en la Nube no es meramente complementaria; es fundamentalmente simbiótica. Si los dispositivos IoT actúan como el sistema nervioso del mundo digital, recopilando datos sensoriales del entorno físico, la nube funciona como su cerebro y su memoria centralizada, proporcionando la capacidad de almacenamiento, procesamiento y análisis a una escala que sería imposible de lograr de otra manera.[34]

Los miles de millones de dispositivos IoT generan un flujo incesante y masivo de datos, a menudo denominado *Big Data*. Gestionar este volumen de datos requiere una infraestructura que sea elástica, escalable y accesible globalmente, características que son la esencia misma de la computación en la nube.[5] La predicción realizada en 2015 por IDC, que estimaba que más del 90% de los datos de IoT serían alojados en la nube en un plazo de cinco años, ha demostrado ser notablemente precisa.[1] Con las proyecciones actuales indicando que la mitad de todos los datos globales residirán en la nube para 2025, y dado que IoT es uno de los principales generadores de nuevos datos, la nube se ha consolidado como el destino de facto para los datos de IoT.[8]

Sin embargo, la arquitectura de IoT está evolucionando más allá de un modelo puramente centralizado. El envío de todos los datos brutos a la nube para su procesamiento introduce desafíos de latencia, costos de ancho de banda y puntos únicos de fallo. Para abordar esto,

ha surgido un paradigma complementario crucial: el **Edge Computing** (computación en el borde). El Edge Computing se refiere al procesamiento de datos en o cerca de la fuente de su generación, es decir, en los propios dispositivos IoT o en puertas de enlace locales, en lugar de enviarlos a un centro de datos centralizado.[25]

La relación no es "Edge vs. Cloud", sino una colaboración estratégica "Edge y Cloud".[37] Esta arquitectura distribuida e inteligente funciona en una jerarquía de tres niveles:

1. **El Dispositivo (Device):** Realiza la captura de datos y, en dispositivos más potentes, puede ejecutar tareas de inferencia de IA simples.
2. **El Borde (Edge):** Una puerta de enlace local o un micro-centro de datos realiza tareas de pre-procesamiento, filtrado de datos, agregación y ejecución de análisis en tiempo real. Esto es crítico para aplicaciones que requieren una respuesta de baja latencia, como el control de maquinaria industrial o las decisiones de un vehículo autónomo, donde esperar una respuesta de la nube sería demasiado lento.[34]
3. **La Nube (Cloud):** Recibe los datos ya filtrados y agregados del borde para el almacenamiento a largo plazo, el análisis de *Big Data* a gran escala y, de manera crucial, el entrenamiento de modelos complejos de inteligencia artificial y aprendizaje automático. Estos modelos entrenados pueden luego ser desplegados de nuevo en el borde para mejorar la inteligencia local.[25]

Este modelo híbrido optimiza el sistema en su conjunto: reduce la latencia para acciones críticas, conserva el ancho de banda al enviar solo datos relevantes a la nube, mejora la resiliencia al permitir que el sistema funcione parcialmente incluso si se pierde la conexión a la nube, y respeta la privacidad al procesar datos sensibles localmente. Por lo tanto, el futuro de la infraestructura de IoT no es una nube monolítica y centralizada, sino una red de computación distribuida e inteligente, donde el procesamiento ocurre en el lugar más eficiente y efectivo para cada tarea.

3.2. Proyecciones de Mercado y Tendencias Convergentes

El crecimiento proyectado para los mercados de Cloud Computing e Internet de las Cosas durante el resto de la década es extraordinariamente robusto, impulsado por la continua transformación digital en todas las industrias. El análisis de diversas fuentes de mercado proporciona una visión cuantitativa de esta expansión.

Proyecciones para Cloud Computing (2025-2030):

- El mercado global de computación en la nube está proyectado para superar los 1.29 billones de dólares en 2025, creciendo hasta alcanzar aproximadamente 2.28 billones de dólares para 2030, lo que representa una Tasa de Crecimiento Anual Compuesta (CAGR)

del 12.0%.[14]
- Otras proyecciones son aún más optimistas, estimando que el mercado podría alcanzar los 1.6 billones de dólares para 2030 con una CAGR del 17.2%.[16] Esta variación puede atribuirse a diferentes metodologías y a la inclusión de distintos segmentos del mercado.
- El gasto de los usuarios finales en servicios de nube pública se espera que alcance los 723.4 mil millones de dólares en 2025.[15]
- Geográficamente, América del Norte sigue siendo el mercado más grande, pero la región de Asia-Pacífico muestra la tasa de crecimiento más rápida, impulsada por la rápida digitalización y el apoyo gubernamental.[14]

Proyecciones para Internet de las Cosas (2025-2030):

- El número de dispositivos IoT conectados a nivel mundial continuará su crecimiento exponencial, con estimaciones que varían entre 30 mil millones y más de 40 mil millones de dispositivos para el año 2030.[24]
- El valor del mercado global de tecnología IoT se proyecta que alcance los 1.14 billones de dólares para 2030.[38]
- El crecimiento en regiones emergentes es particularmente notable. Se espera que el mercado de IoT en América del Sur crezca a una CAGR del 24.3% entre 2023 y 2030, impulsado por la adopción en sectores como la agricultura, la minería y las ciudades inteligentes.[39]

Más allá de las cifras de crecimiento individuales, la tendencia más significativa y transformadora es la **convergencia de Cloud, IoT e Inteligencia Artificial (IA)**. Esta tríada tecnológica forma un ciclo virtuoso que está redefiniendo la innovación:

1. **IoT** recopila los datos masivos del mundo real.
2. **Cloud** proporciona la infraestructura escalable para almacenar estos datos y la potencia de cómputo necesaria para procesarlos.
3. **IA y Machine Learning (ML)**, ejecutándose en la nube, analizan estos datos para encontrar patrones, hacer predicciones y tomar decisiones inteligentes y automatizadas.[25]

Esta sinergia es el motor detrás de las aplicaciones más avanzadas, desde el mantenimiento predictivo en la industria hasta los diagnósticos médicos asistidos por IA y los vehículos autónomos. La capacidad de la nube para democratizar el acceso a herramientas de IA sofisticadas permite a las organizaciones de todos los tamaños extraer un valor inmenso de sus datos de IoT. Esta convergencia no es una tendencia futura; es la realidad operativa que impulsará la próxima ola de ventajas competitivas y disrupción en el mercado.

3.3. Recomendaciones Estratégicas para la Adopción e

Implementación

Para que las organizaciones naveguen con éxito en el complejo y dinámico panorama de la computación en la nube y el IoT, y para que puedan capitalizar plenamente su potencial transformador, es esencial adoptar un enfoque estratégico y holístico. Basado en el análisis exhaustivo de las tecnologías, los mercados y los desafíos, se proponen las siguientes recomendaciones estratégicas:

1. **Adoptar un Enfoque de "Seguridad por Diseño" (*Security by Design*):** La seguridad no puede ser una ocurrencia tardía o un complemento añadido al final del proceso de desarrollo. Debe estar integrada en cada fase del ciclo de vida de un producto o servicio de IoT, desde la concepción y el diseño del hardware hasta el desarrollo del software, el despliegue y el mantenimiento continuo. Esto implica seleccionar componentes de hardware con características de seguridad integradas, implementar un ciclo de vida de desarrollo de software seguro (Secure SDLC), y planificar desde el principio mecanismos robustos para la gestión de identidades y las actualizaciones de firmware seguras.[30]
2. **Diseñar para la Escalabilidad y la Resiliencia:** Las soluciones de IoT deben ser diseñadas desde el principio para escalar y gestionar potencialmente miles de millones de dispositivos y billones de mensajes. Esto requiere el uso de arquitecturas nativas de la nube, como los microservicios y la computación sin servidor, que pueden escalar de forma automática y rentable. Además, la resiliencia debe ser una prioridad, utilizando múltiples zonas de disponibilidad o regiones geográficas en la nube y diseñando sistemas que puedan tolerar fallos de red o de componentes individuales sin una interrupción completa del servicio.[25]
3. **Desarrollar una Estrategia de Datos Cohesiva y Centrada en el Valor:** El verdadero valor de IoT no reside en los dispositivos, sino en los datos que generan. Las organizaciones deben desarrollar una estrategia de datos clara que defina qué datos se recopilarán, cómo se procesarán (en el borde o en la nube), dónde se almacenarán y, lo más importante, cómo se analizarán para generar conocimientos que impulsen los objetivos de negocio. Esto implica invertir en plataformas de análisis de datos, herramientas de IA/ML y talento con habilidades en ciencia de datos para transformar los datos brutos en inteligencia procesable.[5]
4. **Invertir en Talento, Gobernanza y Gestión Financiera:** La tecnología por sí sola no es suficiente. El éxito en la adopción de la nube y el IoT depende críticamente del capital humano y de los marcos de gobernanza. Las organizaciones deben invertir en la capacitación y contratación de personal con habilidades especializadas en áreas como la ciberseguridad de IoT, la arquitectura de la nube, la ingeniería de datos y, cada vez más, la gestión financiera de la nube (FinOps). Establecer un marco de gobernanza claro que defina roles, responsabilidades, políticas de seguridad y cumplimiento es fundamental para gestionar el riesgo y garantizar que las implementaciones tecnológicas estén alineadas con la estrategia empresarial global. La gestión proactiva de los costos

de la nube debe ser una disciplina continua, no una reacción a facturas inesperadas.

Obras citadas

1. FSID_14_Computacion_en_la_nube_IoT.pdf
2. Ventajas y desventajas de la computación en la nube - Google Cloud, fecha de acceso: octubre 27, 2025, https://cloud.google.com/learn/advantages-of-cloud-computing?hl=es-419
3. 11 ventajas de la nube y cómo funciona - Docusign, fecha de acceso: octubre 27, 2025, https://www.docusign.com/es-mx/blog/razones-para-almacenar-sus-archivos-en-la-nube
4. Iaas, Paas, Saas: ¿cuál es la diferencia? - IBM, fecha de acceso: octubre 27, 2025, https://www.ibm.com/es-es/think/topics/iaas-paas-saas
5. ¿Cómo trabaja IoT y la Nube? - Nephos IT, fecha de acceso: octubre 27, 2025, https://www.nephosit.com/como-trabaja-iot-y-la-nube/
6. ¿Cuáles son los beneficios de la computación en la nube? - IBM, fecha de acceso: octubre 27, 2025, https://www.ibm.com/mx-es/think/topics/cloud-computing-benefits
7. 55 Cloud Computing Statistics for 2025 - Spacelift, fecha de acceso: octubre 27, 2025, https://spacelift.io/blog/cloud-computing-statistics
8. 49 Cloud Computing Statistics You Must Know in 2025 - N2W Software, fecha de acceso: octubre 27, 2025, https://n2ws.com/blog/cloud-computing-statistics
9. Chart: The Big Three Stay Ahead in Ever-Growing Cloud Market | Statista, fecha de acceso: octubre 27, 2025, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/
10. Top IaaS Vendors in 2025: Compare the Best Cloud Infrastructure Providers, fecha de acceso: octubre 27, 2025, https://olive.app/blog/top-iaas-vendors-in-2025/
11. Comparativa de los 5 principales proveedores de servicios en la nube en 2025 - DataCamp, fecha de acceso: octubre 27, 2025, https://www.datacamp.com/es/blog/top-cloud-service-providers-compared
12. Los mejores proveedores de IaaS y PaaS - Back4App Blog, fecha de acceso: octubre 27, 2025, https://blog.back4app.com/es/los-mejores-proveedores-de-iaas-y-paas/
13. What are the Top 15 PaaS Providers of 2025? - DevTeam.Space, fecha de acceso: octubre 27, 2025, https://www.devteam.space/blog/paas-providers/
14. Cloud Computing Market Size, Share, Forecast [2030] - MarketsandMarkets, fecha de acceso: octubre 27, 2025, https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html
15. 300+ Cloud Computing Statistics (October- 2025) - Brightlio, fecha de acceso: octubre 27, 2025, https://brightlio.com/cloud-computing-statistics/
16. Cloud Computing on the Rise: Market Projected to Reach $1.6 Trillion by 2030,

fecha de acceso: octubre 27, 2025, https://www.bccresearch.com/pressroom/ift/cloud-computing-market-projected-to-reach-$16-trillion
17. Virtualización. Hipervisores más importantes - Dade2 Spain, fecha de acceso: octubre 27, 2025, https://es.dade2.net/virtualizacion-hipervisores-mas-importantes/
18. Optimizing Virtual Environments: Best 10 Server Virtualization Software in 2025, fecha de acceso: octubre 27, 2025, https://www.cloudnuro.ai/blog/optimizing-virtual-environments-best-10-server-virtualization-software-in-2025
19. Which Hypervisor to Choose in 2025? | Servermall Blog, fecha de acceso: octubre 27, 2025, https://servermall.com/blog/which-hypervisor-to-choose-in-2025/
20. Top 5 Hypervisors of 2025! - YouTube, fecha de acceso: octubre 27, 2025, https://www.youtube.com/shorts/eJcKDxABwe4
21. 90+ Cloud Computing Statistics: A 2025 Market Snapshot - CloudZero, fecha de acceso: octubre 27, 2025, https://www.cloudzero.com/blog/cloud-computing-statistics/
22. ¿Qué es la seguridad de IoT? | Definición y beneficios - Zscaler, fecha de acceso: octubre 27, 2025, https://www.zscaler.com/es/zpedia/what-iot-security
23. IoT market forecast to 2030: connections by region and vertical | GSMA Intelligence, fecha de acceso: octubre 27, 2025, https://www.gsmaintelligence.com/research/iot-market-forecast-to-2030-connections-by-region-and-vertical
24. State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally, fecha de acceso: octubre 27, 2025, https://iot-analytics.com/number-connected-iot-devices/
25. ¿Qué es IoT? - Explicación del Internet de las cosas - AWS, fecha de acceso: octubre 27, 2025, https://aws.amazon.com/es/what-is/iot/
26. ¿Qué es el IoT (IoT)? Definición, beneficios y desafíos - Fortinet, fecha de acceso: octubre 27, 2025, https://www.fortinet.com/lat/resources/cyberglossary/iot
27. Tamaño y alcance del mercado de IoT (2023-2030) - The Insight Partners, fecha de acceso: octubre 27, 2025, https://www.theinsightpartners.com/es/reports/internet-of-things-iot-market
28. ¿Qué es la seguridad del IoT? | Seguridad de los dispositivos IoT - Cloudflare, fecha de acceso: octubre 27, 2025, https://www.cloudflare.com/es-es/learning/security/glossary/iot-security/
29. En 2030 habrá más de 30 billones de dispositivos IoT conectados - Cosmikal, fecha de acceso: octubre 27, 2025, https://www.cosmikal.es/riesgos-dispositivos-iot-conectados/
30. Seguridad de dispositivos IoT : Riesgos, buenas prácticas y consejos de protección, fecha de acceso: octubre 27, 2025, https://www.keyfactor.com/es/education-center/iot-device-security/
31. Seguridad en IoT: Desafíos y Estrategias para Proteger Dispositivos Conectados | SEIDOR, fecha de acceso: octubre 27, 2025, https://www.seidor.com/es-sv/blog/seguridad-iot-desafios-estrategias

32. Seguridad IoT: Definición, Amenazas y Estrategias de Protección - Splashtop, fecha de acceso: octubre 27, 2025, https://www.splashtop.com/es/blog/iot-security
33. Las prácticas de seguridad del Internet de las cosas (IoT) pueden evitar violaciones, fecha de acceso: octubre 27, 2025, https://www.dashlane.com/es/blog/iot-security-breaches
34. IoT y Cloud: ¿Cómo colaboran entre sí? | Blog de Arsys, fecha de acceso: octubre 27, 2025, https://www.arsys.es/blog/iot-cloud
35. El Internet de las Cosas y la Nube - Revista Cloud Computing, fecha de acceso: octubre 27, 2025, https://www.revistacloudcomputing.com/2019/05/__trashed-2/
36. IoT & Cloud Computing - XalDigital, fecha de acceso: octubre 27, 2025, https://www.xaldigital.com/blog/iot-cloud-computing/
37. Edge Computing vs Cloud Computing: Diferencias y relación - Digi International, fecha de acceso: octubre 27, 2025, https://es.digi.com/blog/post/edge-computing-vs-cloud-computing
38. El mercado global de IoT alcanzará los 1,14 billones de dólares en 2030, fecha de acceso: octubre 27, 2025, https://internetdelascosas.xyz/articulo.php?id=11068&titulo=-
39. Crecimiento del mercado de Internet of Things (IoT) de América del Sur [2030], fecha de acceso: octubre 27, 2025, https://www.fortunebusinessinsights.com/es/south-america-internet-of-things-iot-market-107393
40. El impacto de la nube en el IoT y OT - Ikusi, fecha de acceso: octubre 27, 2025, https://www.ikusi.com/mx/blog/nube-en-el-iot/
41. Integrando dispositivos IoT con la nube: mejores prácticas y casos de uso - SEIDOR, fecha de acceso: octubre 27, 2025, https://www.seidor.com/es-es/blog/integrando-dispositivos-iot-nube