EST. 2021 EMC
EDITORIAL MAR CARIBE

TECNOLOGÍAS EMERGENTES EN INGENIERÍA DE SISTEMAS

Ledy Milca Villacrez Mozombite
Norberto Ulises Roman Concha
Javier Elmer Cabrera Díaz
Oscar Benito Pacheco
Frida Mereyda López Córdova
Mario Bernabe Chauca Saavedra
Juan Carlos Lázaro Guillermo

www.editorialmarcaribe.es

ISBN: 978-9915-698-79-3

Tecnologías emergentes en ingeniería de sistemas

Villacrez Mozombite, Ledy Milca; Román Concha, Norberto Ulises; Cabrera Díaz, Javier Elmer; Benito Pacheco, Oscar; López Córdova, Frida Mereyda; Chauca Saavedra, Mario Bernabe; Lázaro Guillermo, Juan Carlos

Primera edición (1.ª ed.): marzo, 2026

Editado por:
Editorial Mar Caribe ®
www.editorialmarcaribe.es
Av. Gral. Flores 547, 70000 Col. del Sacramento, Departamento de Colonia, Uruguay.

Diseño de carátula e ilustraciones: *Luisa Fernanda Lugo Rojas*

Libro electrónico disponible en:
https://editorialmarcaribe.es/ark:/10951/isbn.9789915698793
Formato: Electrónico
ISBN: 978-9915-698-79-3
ARK:
ark:/10951/isbn.9789915698793

Editorial Mar Caribe (OASPA): Como miembro de la Open Access Scholarly Publishing Association, apoyamos el acceso abierto de acuerdo con el código de conducta, la transparencia y las mejores prácticas de OASPA para la publicación de libros académicos y de investigación. Estamos comprometidos con los más altos estándares editoriales en ética y deontología, bajo la premisa de «Ciencia Abierta en América Latina y el Caribe»

OASPA

Editorial Mar Caribe, firmante Nº 795 de 12.08.2024 de la Declaración de Berlín
"... Nos sentimos obligados a abordar los retos de Internet como medio funcional emergente para la distribución del conocimiento. Obviamente, estos avances pueden modificar significativamente la naturaleza de la publicación científica, así como el actual sistema de garantía de calidad...." (Max Planck Society, ed. 2003, pp. 152-153).

Editorial Mar Caribe

Tecnologías emergentes en ingeniería de sistemas

Colonia, Uruguay
2026

Tecnologías emergentes en ingeniería de sistemas

Índice

Introducción

La ingeniería de sistemas está en medio de una transformación sin precedentes. Lo que hace una década parecía ciencia ficción —como que las máquinas pudieran razonar de manera autónoma o que los objetos cotidianos estuvieran interconectados globalmente— hoy es la infraestructura esencial sobre la que se construye la sociedad moderna. Este libro, titulado "Tecnologías emergentes en ingeniería de sistemas", responde a la necesidad de analizar, organizar y prever el impacto de las innovaciones que están redefiniendo la computación y la ingeniería.

En el marco de la Cuarta Revolución Industrial (Industria 4.0), la ingeniería de sistemas ha evolucionado de ser una disciplina centrada únicamente en el desarrollo de software a desempeñar el papel de coordinadora de ecosistemas complejos, inteligentes y resilientes. Este libro analiza la integración de paradigmas como la Inteligencia Artificial (IA) avanzada, el Edge Computing, la seguridad descentralizada basada en Blockchain y la inminente computación cuántica. A través de sus capítulos, el lector encontrará un análisis detallado que conecta la teoría académica con la práctica industrial y ofrece una visión completa de los retos y oportunidades que estas tecnologías plantean para los futuros profesionales.

La rapidez con la que surgen nuevas tecnologías suele superar la capacidad de los programas académicos y las regulaciones para mantenerse al día. Esto genera una demanda urgente de recursos bibliográficos que no solo expliquen las herramientas, sino que también analicen su integración en los sistemas, las consideraciones éticas y su sostenibilidad económica. Dado

que las tecnologías de la información tienen un ciclo de vida breve, este libro ofrece un panorama actualizado que abarca tendencias que aún no figuran en los libros de texto tradicionales.

A diferencia de los manuales técnicos especializados en una única herramienta, esta obra adopta una perspectiva de ingeniería de sistemas y examina cómo la integración de varias tecnologías emergentes impacta la estructura general de los sistemas de información. Para las organizaciones y los ingenieros en formación, entender estas tecnologías no es opcional; es esencial para la innovación y la supervivencia en un mercado cada vez más globalizado y digitalizado.

Hay una creciente preocupación por el consumo energético de los centros de datos y por los sesgos en los algoritmos de IA. Este libro justifica su relevancia al proponer una ingeniería de sistemas verde y responsable, alineada con los Objetivos de Desarrollo Sostenible (ODS). "Tecnologías emergentes en ingeniería de sistemas" es un compendio técnico-analítico dirigido a estudiantes de pregrado y posgrado, investigadores y líderes tecnológicos (CTOs) que desean explorar las fronteras de la computación actual.

El objetivo de esta investigación es analizar y sistematizar el impacto, las aplicaciones y los desafíos de las tecnologías disruptivas actuales en ingeniería de sistemas, proporcionando un marco teórico-práctico que fomente soluciones innovadoras y eficientes para afrontar los problemas complejos de la sociedad digital moderna. Así, el lector obtendrá una perspectiva de la ingeniería de sistemas que prioriza la eficiencia técnica y se dedica a impulsar la transformación social en Latinoamérica, proponiendo un modelo de innovación que, por naturaleza, es inclusivo, ético y profundamente arraigado

en nuestra realidad geográfica y económica.

En este sentido, se invita a los lectores a promover marcos de ciberseguridad y de gobernanza de datos que cumplan con las normativas vigentes y protejan a los ciudadanos en el ecosistema digital regional. Además, se fomenta una cultura de investigación y desarrollo (I+D) que impulse la creación de software soberano y de soluciones de ingeniería con identidad propia, reduciendo así la dependencia tecnológica global.

Capítulo 1
El ecosistema de la ingeniería de sistemas

El panorama de la ingeniería de sistemas se caracteriza por una profunda transformación estructural, impulsada por la necesidad de gestionar una complejidad sistémica sin precedentes en sectores que abarcan desde la infraestructura crítica hasta la salud digital. Esta evolución no es meramente incremental; representa un cambio de paradigma en la forma en que los sistemas se conciben, se diseñan, se operan y se mantienen a lo largo de su ciclo de vida. La transición de un enfoque tradicional basado en documentos hacia un modelo de ingeniería digital centralizado en modelos (MBSE) y gemelos digitales (Digital Twins) ha permitido a las organizaciones establecer hilos digitales (Digital Threads) que actúan como la única fuente de verdad para sistemas de sistemas cada vez más autónomos y adaptativos.

En este contexto, la ingeniería de sistemas se enfrenta al desafío de integrar disciplinas tradicionalmente aisladas, como la mecánica, la electrónica y el software, bajo un marco de inteligencia artificial (IA) que ya no solo automatiza procesos, sino que también razona e interactúa de manera intuitiva con el mundo físico. La madurez de la IA física, la consolidación de SysML v2, la computación en el borde (Edge Computing) de baja latencia y el uso de la blockchain para garantizar la integridad de los datos son los pilares de esta nueva era tecnológica (Alnaim y Alwakeel, 2025).

La Revolución de la Inteligencia Artificial: De la Automatización a los Sistemas Agénticos y Físicos

La inteligencia artificial ha dejado de ser una herramienta de apoyo y se ha convertido en el núcleo operativo de la ingeniería de sistemas. El mercado ha experimentado un cambio desde los pilotos experimentales hacia un despliegue masivo de IA como servicio (AIaaS), en el que las empresas evalúan a los proveedores no solo por sus capacidades de procesamiento, sino también por su eficiencia en la inferencia y su capacidad para integrarse en flujos de trabajo agénticos. El 98% de las organizaciones de servicios empresariales globales ya están desplegando o planean desplegar IA generativa (GenAI) y esperan que esta tecnología transforme profundamente funciones que van desde el servicio al cliente hasta la planificación financiera.

IA Física y el Cierre de la Brecha de Realidad

Uno de los avances más disruptivos es la IA física, que representa la fusión de la inteligencia computacional con el hardware físico para permitir que los agentes inteligentes perciban y actúen en entornos dinámicos e inestructurados. Mediante el aprendizaje por refuerzo y técnicas de transferencia de simulación a realidad (sim-to-real), los ingenieros pueden entrenar sistemas robóticos en entornos virtuales fotorealistas y físicamente precisos antes de su despliegue en el mundo real. Este enfoque ha reducido significativamente la brecha de realidad, permitiendo que brazos robóticos en líneas de ensamblaje o en sistemas de picking en almacenes manipulen

objetos que nunca antes habían manipulado, ajustando su fuerza y su enfoque a partir de retroalimentación visual y táctil en tiempo real.

La IA física utiliza motores físicos avanzados y plataformas de gemelos digitales para crear entornos de entrenamiento sintético a gran escala. Esto permite la generación ilimitada de datos etiquetados que representan diversos escenarios físicos, superando las limitaciones de la recolección de datos en el mundo real (Zhihan, 2023). Además, el avance de los chips de computación en el borde permite realizar este procesamiento directamente en el punto de acción, eliminando la latencia de la comunicación con la nube.

Sistemas Agénticos como Capa Operativa

La interfaz dominante ha pasado de aplicaciones y navegadores aislados a un entorno único nativo de IA. Los sistemas agénticos se han convertido en la capa operativa en la que los flujos de trabajo se colapsan en una corriente personalizada y continua que anticipa y ejecuta transacciones mediante diversas modalidades. En este paradigma, los agentes de IA son tratados como identidades con roles asignados, permisos basados en el principio de menor acceso y monitoreo de la actividad similar al uso humano de los sistemas.

Ingeniería Digital y el Triunfo de MBSE y SysML v2

El Modelado de Sistemas Basado en Modelos (MBSE) se ha consolidado como la base de la ingeniería digital, proporcionando un entorno unificado que

reemplaza la documentación estática por modelos dinámicos. Esta metodología permite gestionar la complejidad de los sistemas contemporáneos, como las ciudades inteligentes y los satélites, que funcionan como sistemas de sistemas integrados.

El Impacto Transformador de SysML v2

El estándar SysML v2 ha marcado un hito en la ingeniería de sistemas al ofrecer mayor precisión, rigor e interoperabilidad en comparación con su predecesor. Construido sobre la base lógica de Kernel Modeling (KerML), SysML v2 permite un enfoque de modelo como código mediante una sintaxis textual completa, lo que facilita la automatización, el control de versiones y la colaboración entre equipos distribuidos a nivel global.

La interoperabilidad se ha visto reforzada por la estandarización de una API basada en HTTP/JSON, que permite el intercambio de modelos sin las complicaciones históricas asociadas al formato XMI. Esto facilita la creación de ecosistemas de ingeniería digital en los que las herramientas de distintos proveedores pueden comunicarse de forma fluida, manteniendo la trazabilidad a lo largo del hilo digital (Nativi et al., 2021).

Casos de Aplicación: Salud y Aeroespacial

En el sector de la tecnología médica (MedTech), el uso de MBSE permite crear un cerebro compartido para el equipo de diseño, documentando no solo lo que hace el sistema, sino también el razonamiento detrás de las decisiones de arquitectura. Por ejemplo, en el desarrollo de sistemas de monitoreo de pacientes, un cambio propuesto en un sensor puede generar automáticamente

alertas de impacto en todos los subsistemas dependientes, desde el software hasta los protocolos de validación regulatoria. Esto reduce los procesos que antes tomaban semanas a solo unos pocos días de análisis de impacto digital.

En el ámbito aeroespacial y de defensa, el Departamento de Defensa de los Estados Unidos ha hecho de MBSE un pilar de su estrategia de ingeniería digital para acelerar el desarrollo de sistemas complejos y mitigar riesgos de integración de forma temprana. El uso de simulaciones avanzadas permite validar diseños antes de construir hardware físico, aplicando el principio de shift left para identificar errores costosos en las etapas iniciales del ciclo de vida.

Computación en el Borde (Edge Computing) e Internet de las Cosas (IoT) masivo

La arquitectura de sistemas ha migrado de un modelo centralizado en la nube a uno descentralizado en el borde para abordar los desafíos de latencia, ancho de banda y soberanía de datos. El despliegue de aproximadamente 21 mil millones de dispositivos IoT exige que el procesamiento de datos se realice lo más cerca posible de la fuente.

Inferencia Local y Reducción de Costos

La computación en el borde permite realizar inferencia de IA localmente, filtrando el ruido de los datos de telemetría y transmitiendo solo la información accionable a los sistemas centrales. Se estima que esta estrategia reduce en un 80% los costos promedio de transporte de datos

(backhaul). En aplicaciones de fabricación inteligente, los gateways de borde industriales permiten respuestas en milisegundos, esenciales para el control de brazos robóticos o de sistemas de seguridad en subestaciones eléctricas.

Arquitectura de Gateway de Borde Industrial

Los dispositivos de borde modernos, como el Robustel EG5120, están equipados con hardware de alto rendimiento para satisfacer las demandas actuales. Estas unidades incluyen procesadores multinúcleo con unidades de procesamiento neural (NPU) dedicadas a acelerar cargas de trabajo de aprendizaje automático para visión artificial o detección de anomalías.

El uso de contenedores (Docker) en el borde permite desacoplar el software del hardware, facilitando el despliegue de microservicios y de analítica compleja mediante flotas globales de gateways con un único comando. Además, estas arquitecturas proporcionan autonomía operativa: si falla la conexión a Internet, el gateway local mantiene los bucles de control críticos y almacena los datos localmente hasta que se restablezca la conexión.

Ciberseguridad por Diseño y el Rol de Blockchain en la Integridad de Sistemas

La ciberseguridad ya no se añade de forma retrospectiva, sino que forma parte integral de la arquitectura del sistema (Security by Design). Con el aumento de las amenazas potenciadas por la IA y la fragmentación geopolítica, la resiliencia digital se ha convertido en una prioridad de nivel ejecutivo (Salem et al., 2024).

Confianza Cero y Visibilidad de la Cadena de Suministro

Las organizaciones han adoptado modelos de Confianza Cero (Zero Trust),en los que cada identidad y cada acceso se verifican continuamente. La visibilidad de la cadena de suministro es crítica, ya que se prevé que las vulnerabilidades de los proveedores externos representen el 45% de los incidentes de seguridad a nivel global (Xu et al., 2025). El uso de listas de materiales de software (SBOM) permite rastrear cada componente y cada biblioteca de código abierto en cada compilación, lo que permite detectar de forma proactiva manipulaciones o dependencias obsoletas.

Blockchain para la Trazabilidad y la Propiedad Intelectual

La tecnología blockchain se utiliza para crear registros inmutables de la historia de los materiales y de los procesos. Por ejemplo, en el comercio global, se incrustan firmas moleculares únicas en materiales físicos (plásticos, metales, combustibles) que se vinculan a un registro seguro en la blockchain, creando un hilo digital permanente y resistente a la manipulación.

En la fabricación aditiva (3D printing), plataformas basadas en blockchain como Autentica protegen la propiedad intelectual al cifrar los archivos de diseño y al crear trazabilidad para la gestión segura de los activos digitales en cadenas de suministro distribuidas. Esto permite que incluso los pequeños fabricantes compartan diseños con confianza, sabiendo que su IP está protegida mediante protocolos de cifrado y verificación descentralizada.

Computación Cuántica y Optimización de Sistemas Complejos

La computación cuántica ha entrado en una fase de uso empresarial aplicado, resolviendo problemas que resultan computacionalmente intratables para los sistemas clásicos. Aunque todavía enfrentamos limitaciones de ruido y decoherencia, los sistemas híbridos clásico-cuánticos están demostrando ventajas medibles en optimización, simulación y descubrimiento científico.

Avances en Optimización Cuántica

La optimización cuántica utiliza principios como la superposición y el entrelazamiento para navegar por espacios de soluciones masivos de forma simultánea. En logística, las empresas están utilizando algoritmos cuánticos para optimizar rutas de entrega en tiempo real, logrando mejoras del 10% al 20% en la eficiencia de las flotas, lo que se traduce en ahorros significativos de combustible y tiempo.

En finanzas, los bancos experimentan con algoritmos cuánticos para la optimización de carteras y la detección de fraude, reduciendo los tiempos de cálculo de horas a minutos. Los procesadores cuánticos cuentan con entre 50 y 1.000 qubits, dependiendo de la arquitectura, aunque la fidelidad de las puertas sigue siendo un desafío técnico que requiere estrategias de mitigación de errores.

Simulación de Fluidos y Materiales

Un hito notable es la aplicación de Redes Neuronales Informadas por la Física Conscientes de lo Cuántico (QA-PINN) a la Dinámica de Fluidos Computacional (CFD), lo que logra una aceleración de 25 veces en el entrenamiento de simulaciones complejas. Además, la colaboración entre líderes de la industria ha logrado una compresión de circuitos de 100X para QCFD, lo que facilita el diseño de aeronaves y sistemas de energía más eficientes. Ingeniería de Sistemas Sostenible y Economía Circular

La sostenibilidad se ha transformado de una iniciativa aislada en una disciplina de ingeniería central, impulsada por la necesidad de reducir costos operativos y de cumplir con regulaciones climáticas estrictas. Las organizaciones están aplicando el pensamiento sistémico, liderado por el diseño, para integrar la circularidad desde las primeras etapas del desarrollo del producto (Bautista, 2019).

Circularidad por Diseño y Gemelos Digitales

El uso de gemelos digitales permite a los equipos de ingeniería modelar los ciclos de vida completos de los productos y evaluar el impacto ambiental de los materiales antes de que comience la producción física. Esto facilita la planificación de la reutilización, el reacondicionamiento y el reciclaje al final de la vida útil, manteniendo los materiales en circulación más tiempo y reduciendo el desperdicio (Chaparro et al., 2025).

Innovación en Energía y Microgrids

La ingeniería sostenible está escalando desde pilotos hasta

infraestructuras de gran escala, como edificios inteligentes y microgrids a nivel de vecindario. El avance en silicio de alto rendimiento, proporciona una mayor eficiencia en vatios por rendimiento, lo que ayuda a modernizar la infraestructura mientras se reduce el consumo energético, un factor crítico a medida que la demanda de electricidad de los centros de datos se triplica debido a las cargas de trabajo de IA (Martinez et al., 2021).

Evolución de las Competencias Profesionales y el Perfil del Ingeniero

La transformación tecnológica exige una evolución paralela del capital humano. El ingeniero de sistemas moderno debe ser un pensador holístico que combine una profunda fluidez digital con habilidades de liderazgo técnico y ética profesional.

El Marco de Competencias de INCOSE 2035

El Consejo Internacional de Ingeniería de Sistemas (INCOSE) ha definido competencias clave que incluyen no solo la arquitectura y el diseño técnico, sino también la dinámica de equipos, la inteligencia emocional y el coaching. Los ingenieros deben ser capaces de navegar por plataformas en la nube, analizar grandes volúmenes de datos y colaborar virtualmente en ecosistemas de ingeniería digital (Nativi et al., 2021). Las habilidades en alta demanda incluyen:

- **Ingeniería de Plataformas:** Evolución de DevOps para crear entornos en los que los desarrolladores puedan autoservirse de infraestructura y

herramientas.**DevSecOps y GitOps:** automatización de la seguridad y del mantenimiento de sistemas en sincronía con los cambios de código.

- **FinOps:** gestión de costos en la nube para evitar el sobregasto de recursos de IA.
- **Sistemas de Sistemas (SoS):** Capacidad para integrar componentes de software, electrónica y sensores en ecosistemas vastos y autónomos.

La ingeniería de sistemas se encuentra en una encrucijada en la que la tecnología y la estrategia de negocio son inseparables. La capacidad de integrar la IA física con modelos digitales precisos (MBSE) y de garantizar la integridad de los datos mediante blockchain no es solo una ventaja competitiva, sino un requisito para la supervivencia en un mercado global fragmentado y volátil (López et al., 2024).

La transición hacia sistemas autónomos, adaptativos y sostenibles requiere una visión a largo plazo en la que la seguridad por diseño y la circularidad no sean añadidos, sino principios fundamentales del ciclo de vida del sistema. Los ingenieros que logren dominar este ecosistema digital, aprovechando la potencia de la computación cuántica y de la computación en el borde, serán los arquitectos de las infraestructuras críticas que definirán la resiliencia y el crecimiento de la sociedad en las décadas venideras.

En última instancia, el éxito de estos sistemas complejos dependerá de la creación de un hilo digital resiliente y transparente, que permita a los humanos y a la IA colaborar de manera efectiva en la resolución de los desafíos más apremiantes de nuestro tiempo.

Capítulo 2

Estrategias avanzadas en el internet de las cosas para la creación de entornos inteligentes y la transformación digital de la industria

La convergencia tecnológica que define la tercera década del siglo XXI ha situado al Internet de las Cosas (IoT) no solo como una herramienta de conectividad, sino también como el tejido fundamental de la nueva infraestructura global. Esta arquitectura de interconexión masiva, que integra sensores, actuadores y sistemas de procesamiento avanzado, permite la transición de entornos estáticos a ecosistemas dinámicos y autogestionados (Nativi et al., 2021).

En el ámbito industrial, esta evolución se manifiesta a través del Internet Industrial de las Cosas (IIoT), un subconjunto especializado que prioriza la robustez, la precisión y la seguridad para optimizar procesos críticos en sectores como la manufactura, la energía y la minería. La integración de estas tecnologías facilita una visibilidad sin precedentes de los activos físicos, permitiendo que los datos recolectados se transformen en inteligencia accionable mediante algoritmos de aprendizaje automático y arquitecturas de computación de borde.

Arquitectura y Diferenciación entre IoT y IIoT en la Gestión de Infraestructuras

La distinción entre el IoT orientado al consumidor y el IIoT es fundamental para los profesionales que diseñan soluciones de automatización. Mientras que el IoT de consumo se enfoca principalmente en mejorar la experiencia del usuario y la conveniencia personal mediante dispositivos como termostatos inteligentes y dispositivos vestibles de salud, el IIoT se sitúa en el núcleo de las operaciones de misión crítica. Las exigencias técnicas del entorno industrial demandan una arquitectura capaz de soportar condiciones extremas y de garantizar la continuidad del negocio en cualquier circunstancia.

Dimensiones Críticas de Operación y Rendimiento

Existen cuatro pilares fundamentales en los que el IoT y el IIoT divergen significativamente: seguridad, precisión, fiabilidad y escalabilidad. La seguridad en el entorno IIoT adopta un enfoque de defensa en profundidad, dado que una brecha puede comprometer no solo la propiedad intelectual o los activos financieros, sino también la integridad física de los operarios y la estabilidad de las infraestructuras nacionales. Por el contrario, las soluciones de consumo suelen manejar volúmenes de datos menos críticos, lo que permite utilizar protocolos de seguridad menos rigurosos.

En términos de precisión, las aplicaciones industriales operan a escalas de milisegundos. En una línea de ensamblaje de alta velocidad, la sincronización entre sensores y actuadores debe ser absoluta para evitar fallos de producción que ocasionen pérdidas millonarias. La fiabilidad también es un

factor determinante; mientras que un dispositivo de consumo puede ser reiniciado manualmente por el usuario ante un fallo, los sensores industriales deben operar de forma autónoma durante décadas en entornos hostiles, sujetos a vibraciones extremas, temperaturas variables y presiones elevadas.

Uno de los mayores desafíos en la automatización contemporánea es la integración de los sistemas de Tecnología de la Operación (OT), tradicionalmente aislados, con las infraestructuras de Tecnología de la Información (TI). El mundo OT se caracteriza por el uso de controladores lógicos programables (PLC), sistemas SCADA y robots que priorizan la seguridad física y la disponibilidad inmediata. En contraste, el entorno IT se centra en la gestión de datos, la seguridad lógica y la escalabilidad del software en la nube.

La creación de un puente entre estos dos dominios se logra mediante pasarelas (gateways) industriales inteligentes que traducen protocolos y procesan datos localmente. Esta integración permite que la información fluya desde la planta de producción hacia los sistemas de planificación de recursos empresariales (ERP) y de ejecución de manufactura (MES), creando un bucle de retroalimentación en el que las decisiones comerciales se basan en el estado real y predictivo de la maquinaria física.

Protocolos de Comunicación e Interoperabilidad en la Industria 4.0

La capacidad de intercambio de información entre dispositivos de diferentes fabricantes es el corazón de la Industria 4.0. Para lograr esta

interoperabilidad, se han consolidado estándares que permiten una comunicación fluida y segura (Yaqub y Alsabban, 2023). Entre los protocolos más destacados se encuentran MQTT y OPC UA, cada uno diseñado para satisfacer necesidades específicas del ecosistema industrial.MQTT: Eficiencia y Escalabilidad en la Transmisión de Datos

El protocolo Message Queuing Telemetry Transport (MQTT) se basa en un modelo de publicación y suscripción que utiliza un intermediario (broker) central para gestionar los mensajes. Su diseño ligero, con cabeceras de tan solo 2 bytes, lo hace ideal para redes con ancho de banda limitado o alta latencia, comunes en aplicaciones de monitoreo remoto como oleoductos o parques eólicos. MQTT ofrece tres niveles de Calidad de Servicio (QoS), que van desde el envío de mensajes sin confirmación (QoS 0) hasta la garantía absoluta de entrega mediante mecanismos de almacenamiento y reenvío (QoS 2).

OPC UA: El Estándar para el Modelado Semántico de Información

A diferencia de los protocolos que solo definen el transporte de datos, Open Platform Communications Unified Architecture (OPC UA) es un marco completo que define cómo se estructura y se contextualiza la información. OPC UA utiliza un modelo jerárquico de objetos y variables, lo que permite que una máquina explique a otra no solo un valor numérico, sino también su unidad de medida, su rango de operación y su estado de salud. Esta capacidad semántica es crucial para reducir la complejidad de la integración, ya que los sistemas receptores pueden interpretar automáticamente la relación entre los datos sin

necesidad de programación manual exhaustiva.

La coexistencia de ambos protocolos es cada vez más común en arquitecturas híbridas. El uso de la especificación Sparkplug B sobre MQTT añade una capa de estructura y gestión de estado que acerca la eficiencia de MQTT a la riqueza informativa de OPC UA, facilitando la implementación de lo que se conoce como el Espacio de Nombres Unificado (Unified Namespace).

Arquitecturas de Espacio de Nombres Unificado (UNS) y Gestión de Datos

A medida que las organizaciones escalan sus despliegues de IIoT, la integración tradicional punto a punto se convierte en un obstáculo infranqueable que genera silos de información. El Espacio de Nombres Unificado (UNS) propone un cambio de paradigma hacia una arquitectura basada en eventos, en la que el estado actual del negocio y de la producción se refleja en una única fuente de verdad compartida.

Estructura y Funcionamiento del UNS

El UNS organiza la información siguiendo jerarquías estandarizadas, como la norma ISA-95, que estructura los datos desde el nivel de empresa, sitio, área, línea y, finalmente, celda de producción. Cada dispositivo o sistema actúa como un nodo que publica su estado en esta estructura jerárquica. De este modo, si un sistema de análisis de eficiencia energética necesita datos sobre el consumo de una línea de ensamblaje, simplemente se suscribe al nodo correspondiente en el UNS, sin necesidad de conocer la dirección IP ni

el protocolo específico del PLC original.

Este enfoque democratiza el acceso a los datos en la organización. Por ejemplo, el departamento de finanzas puede acceder a datos de producción en tiempo real para ajustar las previsiones de costos, mientras que el equipo de mantenimiento monitorea los mismos datos para detectar anomalías. El UNS no reside en un software específico, sino que es una construcción lógica implementada típicamente sobre brokers de mensajes de alto rendimiento, como HiveMQ, o sobre plataformas de integración, como Ignition.

Beneficios de la Desacoplación de Sistemas

La implementación de un UNS permite a las empresas industriales alcanzar niveles superiores de agilidad operativa:

- **Reducción de la Complejidad:** Se eliminan las conexiones múltiples entre sistemas, lo que permite que cada nodo requiera una única conexión al broker central para interactuar con todo el ecosistema.
- **Escalabilidad Sin Interrupciones:** La incorporación de nuevos sensores o aplicaciones no requiere reprogramar los sistemas existentes; los nuevos componentes simplemente se conectan al UNS y comienzan a publicar o consumir datos.
- **Base para Digital Twins:** Al proporcionar datos contextualizados y en tiempo real, el UNS es el cimiento necesario para construir gemelos digitales que repliquen con precisión el comportamiento de los activos físicos.
- **Automatización de Procesos de Negocio:** La sincronización entre el ERP y el piso de fábrica permite que la creación de una orden de cliente

dispare automáticamente ajustes en los cronogramas de producción y en los requerimientos de inventario.

El Impacto de 5G y Computación de Borde en la Automatización Industrial

La transición hacia la Industria 4.0 exige capacidades de conectividad que superan las limitaciones de las redes cableadas tradicionales y de las tecnologías inalámbricas de generaciones anteriores. En este escenario, la combinación de redes 5G y computación de borde (Edge Computing) es fundamental para habilitar aplicaciones que requieren una respuesta casi instantánea y el manejo masivo de dispositivos (Yaqub y Alsabban, 2023).

Latencia ultrabaja y confiabilidad en el borde

Las redes 5G ofrecen una mejora disruptiva en términos de latencia, logrando tiempos de respuesta inferiores a 5 milisegundos, frente a los 60-100 milisegundos típicos de las redes 4G. Esta capacidad es crítica para sistemas de control en tiempo real, como la robótica colaborativa (cobots) y los vehículos de guiado automático (AGV). Al procesar los datos en el borde —es decir, en el gateway industrial o en servidores locales cercanos a la fuente— se evita el retraso inherente al traslado de la información a centros de datos remotos en la nube (Krejčí et al., 2025).

Investigaciones recientes demuestran que el procesamiento local puede reducir la latencia de 4,03 ms a 3,03 ms, un margen que, aunque parezca pequeño, es decisivo para la estabilidad de los bucles de control de

alta precisión utilizados en la fabricación de semiconductores o en la sincronización de sistemas de movimiento multieje. Además, el 5G permite la creación de redes privadas (Private Networks), lo que garantiza a las empresas industriales un ancho de banda dedicado y una seguridad superior al aislar sus comunicaciones críticas del tráfico público de internet.

Integración de Inteligencia Artificial en el Borde (Edge AI)

La evolución tecnológica está impulsando el concepto de AIoT (Artificial Intelligence of Things), en el que la inferencia de inteligencia artificial ocurre directamente en el hardware de campo. Dispositivos como la serie ABOX o SBOX de SINTRONES están equipados con procesadores y aceleradores gráficos capaces de ejecutar modelos de visión artificial para el control de calidad o la detección de anomalías, sin depender de la conectividad a la nube. Este enfoque no solo mejora la velocidad de respuesta, sino que también protege la privacidad de los datos y reduce los costos de transferencia de información masiva.

Aplicaciones de Mantenimiento Predictivo y Monitoreo de Activos

Una de las aplicaciones de mayor retorno económico del IIoT es el mantenimiento predictivo (PdM). Tradicionalmente, las empresas han dependido del mantenimiento reactivo (reparar después de la rotura) o preventivo (reparar por calendario), ambos altamente ineficientes. El PdM, apalancado por sensores de IoT y analítica avanzada, permite intervenir en los equipos solo cuando sea estrictamente necesario, en función de su estado real.

Mecanismos de Análisis y Detección de Anomalías

El mantenimiento predictivo opera mediante la recolección continua de datos de series temporales, como vibraciones ultrasónicas, perfiles de temperatura y fluctuaciones del consumo eléctrico. Estos datos alimentan modelos de aprendizaje automático que aprenden los patrones de comportamiento normales de la máquina. Cuando el sensor detecta una desviación mínima —por ejemplo, una vibración imperceptible para el oído humano que indica el inicio del desgaste de un rodamiento—, el sistema emite una alerta predictiva.

Los beneficios cuantificables de estas soluciones son significativos. Según informes sectoriales, el mantenimiento predictivo puede reducir los costos de mantenimiento hasta en un 40% y disminuir el tiempo de inactividad no planificado en un 50%. Además, el PdM contribuye a la sostenibilidad al prolongar la vida útil de los componentes y evitar el reemplazo innecesario de piezas que aún tienen vida útil remanente.

Casos reales de impacto en sectores estratégicos

El despliegue de estas tecnologías ha transformado a líderes industriales globales, proporcionando lecciones valiosas sobre la escala y la ejecución:

- **Caterpillar:** Utiliza una red global de más de 500.000 activos conectados. Sus algoritmos identifican fallos potenciales con semanas de antelación, lo que permite a los clientes ahorrar hasta $400,000 por máquina al año en operaciones mineras al prevenir paradas catastróficas.

- **Ford:** En su planta de Valencia, ha implementado una plataforma que procesa 250 millones de puntos de datos diarios. Esto ha permitido reducir en un 25% los tiempos de inactividad no planificados y mejorar la calidad del producto final, disminuyendo los defectos en un 8%.
- **Harley-Davidson:** logró reducir el ciclo de fabricación de una motocicleta de 21 días a tan solo 6 horas gracias a la monitorización continua de la calidad y a sistemas de programación dinámica basados en IoT.

La creación de entornos inteligentes: Smart Buildings y Smart Cities

Más allá de los muros de la fábrica, el IoT es la tecnología que facilita la creación de infraestructuras sostenibles y resilientes. Los entornos inteligentes utilizan redes de sensores para optimizar el uso de recursos finitos y mejorar la calidad de vida de las poblaciones urbanas.

Sistemas de Gestión de Energía en Edificios Inteligentes (EMS)

Los edificios son responsables de una parte sustancial del consumo energético global. Los sistemas de gestión de energía (EMS) inteligentes abordan este desafío mediante la integración de sensores de ocupación, medidores inteligentes y algoritmos de inteligencia artificial. Estos sistemas detectan ineficiencias en tiempo real, como el funcionamiento de sistemas de climatización (HVAC) en áreas vacías o la iluminación excesiva durante las horas de luz natural.

La implementación de medidores y paneles inteligentes, considerados el cerebro del sistema, permite a los administradores identificar sobrecargas y optimizar las tarifas eléctricas desplazando las operaciones de mayor consumo a horas valle. Además, la integración de recursos energéticos distribuidos, como paneles solares y sistemas de almacenamiento de energía en baterías, permite que los edificios inteligentes no solo consuman energía, sino que también participen activamente en la estabilidad de la red eléctrica mediante estrategias de respuesta a la demanda.

Movilidad y Gestión Urbana en Ciudades Inteligentes

Las ciudades inteligentes representan la aplicación a gran escala del IoT. Mediante Tecnologías de la Información y la Comunicación (TIC), los centros urbanos recopilan datos de sensores ubicados en semáforos, en vehículos de transporte público y en redes de suministro de agua. La movilidad inteligente utiliza el análisis de datos en tiempo real para gestionar el flujo vehicular, reducir la congestión y minimizar las emisiones de CO_2.

Un aspecto crítico es la transición hacia la movilidad sostenible. Las ciudades están implementando infraestructura para vehículos eléctricos (EV) y sistemas integrados de transporte compartido. El uso de redes 5G y, en el futuro, 6G, permitirá que los sistemas urbanos sean aún más reactivos, detectando automáticamente accidentes o fugas en las redes de agua y de aire y ajustando los servicios municipales de forma proactiva.

La Transformación Digital en el Perú: Proyectos Emblemáticos e Industria 4.0.

El Perú está experimentando una aceleración sin precedentes en la adopción de tecnologías de la industria 4.0, impulsada por proyectos de infraestructura de gran escala que integran IoT, 5G e inteligencia artificial en su diseño.

El Puerto de Chancay: Un Referente Regional en Automatización

El Megapuerto de Chancay se ha posicionado como el enclave logístico más automatizado del Pacífico Sur. Este proyecto utiliza tecnología 5G para coordinar una flota de 40 vehículos autónomos y eléctricos que transportan contenedores entre los muelles y el patio de operaciones sin intervención humana.

La integración de gemelos digitales y el análisis de Big Data permiten identificar automáticamente a los buques a gran distancia, optimizar las maniobras de carga y descarga y aumentar la productividad portuaria en un 20% (Zhihan, 2023).

La arquitectura del puerto ha sido diseñada para ser 5G-ready y 6G-ready, lo que permite actualizaciones de red sin necesidad de reemplazar la infraestructura física y asegura la competitividad del terminal a largo plazo. Además, el enfoque en la sostenibilidad convierte a Chancay en un puerto verde, alineado con los objetivos globales de reducción de las emisiones del

transporte marítimo.

Modernización y Expansión del Aeropuerto Internacional Jorge Chávez

La expansión del aeropuerto principal del país es otro ejemplo de la integración de infraestructuras críticas inteligentes. La nueva terminal, operativa desde junio de 2025, cuenta con una superficie de 270,00 m^2 y está equipada con sistemas de ICT de vanguardia. La implementación de biometría y e-gates permite a los pasajeros agilizar su control migratorio mediante el pre-registro en la plataforma Migracheck, reduciendo drásticamente las colas y mejorando la experiencia del usuario.

El proyecto incluye un ecosistema digital robusto, implementado por expertos en tecnología, que garantiza la seguridad y la eficiencia de las operaciones terrestres y aéreas. La visión a largo plazo para el Jorge Chávez es convertirse en una ciudad aeroportuaria que integre logística, negocios y transporte conectado, posicionando a Lima como un hub regional clave frente a Bogotá y São Paulo.

Minería 4.0: Innovación en Quellaveco y Antamina

El sector minero peruano lidera la adopción de la inteligencia artificial y de la automatización masiva. En la mina Quellaveco se ha implementado una estrategia integral de minería digital, en la que la autonomía de la flota de camiones genera un flujo constante de datos analizados en tiempo real mediante dashboards operacionales.El uso de algoritmos para optimizar la carga útil (payload) y reducir los tiempos de ciclo entre palas (bucket-to-

bucket) ha permitido alcanzar récords históricos de producción.

Por otro lado, Antamina ha desarrollado modelos de Machine Learning para predecir y optimizar la recuperación de cobre y zinc. Mediante la extracción de datos de los sistemas de planta, geología y despacho, el equipo de analítica avanzada ha implementado algoritmos que ajustan los parámetros operativos para optimizar el rendimiento metalúrgico con un alto grado de precisión.Estos avances demuestran que la arquitectura de datos es el activo más valioso para la minería del futuro.

Estrategia Nacional de Inteligencia Artificial (ENIA)

El marco normativo y estratégico del Perú se está adaptando para fomentar la innovación tecnológica. La Estrategia Nacional de Inteligencia Artificial busca fortalecer el ecosistema nacional mediante la colaboración público-privada, el desarrollo de talento humano y la promoción de la investigación en IA ética y responsable.

Ejes de Desarrollo e Impacto Socioeconómico

La ENIA identifica sectores estratégicos, como la agricultura, en los que el uso de IA y sensores IoT en el manejo de cultivos puede ahorrar hasta un 50% de agua y energía. En el ámbito de la justicia, se exploran algoritmos para predecir la carga procesal, mientras que en el ámbito educativo se impulsa la personalización del aprendizaje basada en las necesidades de cada estudiante.

Un pilar fundamental de la estrategia es el uso de los datos abiertos como

activos nacionales. Se estima que la correcta implementación de políticas de datos y IA podría impactar significativamente en la creación de empleo, con proyecciones de hasta 1,97 millones de puestos de trabajo vinculados a la economía digital para el cierre de la década. Sin embargo, la estrategia también reconoce desafíos críticos, como la necesidad de proteger la privacidad de los datos personales y garantizar la no discriminación algorítmica mediante la creación de sandboxes regulatorios.

Ciberseguridad en Sistemas de Control Industrial (OT)

La apertura de las redes industriales a internet y su integración con la nube exponen a las organizaciones a riesgos cibernéticos sin precedentes. La seguridad en el entorno OT no es solo una cuestión técnica, sino también una inversión estratégica esencial para garantizar la continuidad operativa de los servicios críticos (Salem et al., 2024).

La norma ISA/IEC 62443: referencia global para la protección OT

El estándar internacional ISA/IEC 62443 proporciona un marco integral para identificar y mitigar vulnerabilidades en los sistemas de automatización y control industrial (IACS). Esta norma promueve el concepto de defensa en profundidad, que consiste en el escalonamiento de mecanismos de seguridad técnicos y organizacionales para dificultar la penetración de un atacante.

Los niveles de seguridad (Security Levels o SL) definidos por la norma

permiten clasificar la protección necesaria:

- **SL 1:** Protección contra infracciones accidentales o errores humanos no maliciosos.
- **SL 2:** Protección contra violaciones intencionales por parte de individuos con medios sencillos y poca motivación.
- **SL 3:** Protección contra ataques sofisticados de adversarios con recursos moderados.
- **SL 4:** Protección contra amenazas avanzadas con recursos estatales o de gran impacto destructivo.

Las organizaciones que operan infraestructuras críticas en Perú, como Luz del Sur o Sedapal, ya están alineando sus centros de control con estos estándares para fortalecer la resiliencia operativa frente a ciberataques sofisticados. La implementación de la segmentación de red en zonas y conductos, así como la supervisión continua mediante herramientas de detección de amenazas basadas en IA, son hoy requisitos obligatorios para cualquier operación industrial moderna.

El despliegue masivo del Internet de las Cosas y la automatización inteligente marcan el inicio de una era de eficiencia y sostenibilidad sin precedentes. A medida que avanzamos hacia 2030, la capacidad de las organizaciones para gestionar la complejidad de los datos y asegurar sus infraestructuras determinará su posición en el mercado global.

1. **La Inteligencia de los Datos como Activo Estratégico:** La mera conectividad ya no constituye un diferencial competitivo. El verdadero valor reside en la capacidad de extraer inteligencia accionable mediante

arquitecturas como el Espacio de Nombres Unificado (UNS), que permite una visibilidad holística del negocio desde el sensor en planta hasta el ERP en la nube.

2. **Convergencia Tecnológica Habilitadora:** La combinación de 5G, computación de borde y AIoT está eliminando las barreras de latencia y de procesamiento que limitaban la automatización en el pasado. El éxito de proyectos como el Puerto de Chancay demuestra que el Perú puede liderar la implementación de estas tecnologías a escala regional.
3. **Mantenimiento Predictivo y Sostenibilidad:** La adopción de estrategias de mantenimiento basadas en datos no solo reduce significativamente los costos operativos, sino que también impulsa la sostenibilidad industrial al optimizar el uso de la energía y al extender la vida útil de los activos físicos.
4. **Resiliencia Mediante Estándares:** La ciberseguridad industrial, basada en normas como la ISA/IEC 62443, debe integrarse desde el diseño (security by design) de cualquier proyecto de IIoT para proteger la integridad de las infraestructuras críticas nacionales.
5. **Desarrollo de Talento y Marco Ético:** La transformación digital exitosa requiere un compromiso con el desarrollo del talento humano y un marco regulatorio que promueva la innovación y, al mismo tiempo, garantice el uso ético y transparente de la inteligencia artificial.

La era del IoT industrial no es una meta final, sino una evolución constante hacia sistemas más autónomos, resilientes y centrados en los datos. El liderazgo en este nuevo paradigma pertenecerá a quienes logren orquestar de manera armónica la tecnología, las personas y los procesos en un

ecosistema digital integrado (Araujo et al., 2024).

Capítulo 3
Estrategia integral de resiliencia para la integridad de los datos

La arquitectura de la confianza digital en la sociedad contemporánea se encuentra en una encrucijada histórica. Durante las últimas décadas, la integridad de los datos en sistemas complejos ha dependido casi exclusivamente de la asimetría computacional que ofrecen los algoritmos criptográficos clásicos. Sin embargo, el surgimiento de la computación cuántica representa un cambio de paradigma que no solo amenaza con invalidar estas defensas, sino que también ofrece herramientas sin precedentes para redefinir la inmutabilidad de la información. La intersección entre la computación cuántica y la cadena de bloques (*blockchain*) constituye uno de los campos de investigación más críticos para la seguridad nacional, la estabilidad financiera y la resiliencia de infraestructuras críticas como la salud y la energía.

El concepto de integridad de los datos, definido como el mantenimiento y la garantía de la exactitud y la consistencia de la información a lo largo de su ciclo de vida, se vuelve infinitamente más difícil de proteger en sistemas complejos en los que múltiples actores interactúan sin una autoridad central. La tecnología de cadena de bloques surgió como respuesta a esta necesidad, proporcionando un registro público, distribuido y resistente a la manipulación. No obstante, los cimientos matemáticos de este registro, que alguna vez se

consideraron inexpugnables, están siendo cuestionados por la capacidad de los ordenadores cuánticos para resolver problemas de factorización y de logaritmos discretos en tiempos que resultan inalcanzables para la informática tradicional.

Fundamentos de la amenaza cuántica sobre los protocolos de registros distribuidos

Para comprender la magnitud de la amenaza, es imperativo analizar los mecanismos mediante los cuales la computación cuántica desmantela la seguridad clásica. Mientras que los ordenadores tradicionales procesan información en bits binarios, los sistemas cuánticos utilizan qubits que aprovechan la superposición y el entrelazamiento, lo que permite una exploración paralela de espacios de soluciones masivos.

El algoritmo de Shor y la ruptura de la criptografía de clave pública

La vulnerabilidad más crítica de las redes de cadena de bloques actuales radica en el algoritmo de Shor. Este procedimiento cuántico permite encontrar los factores primos de un número entero grande de manera exponencialmente más rápida que cualquier algoritmo clásico conocido. Dado que la mayoría de los sistemas de cadena de bloques, incluidos Bitcoin y Ethereum, utilizan el Algoritmo de Firma Digital de Curva Elíptica (ECDSA) o RSA para garantizar que solo el propietario de una cuenta pueda autorizar transacciones, la capacidad de un ordenador cuántico para derivar una clave privada a partir de una pública destruye el concepto de propiedad y

autenticidad.

Aunque los dispositivos actuales aún no han alcanzado esta escala de corrección de errores, la tendencia de optimización sugiere que el horizonte de amenaza es ineludible. El impacto no es solo futuro; existe un riesgo inmediato conocido como Cosechar ahora, descifrar después (SNDL, por sus siglas en inglés), en el que los adversarios interceptan y almacenan datos cifrados hoy con la intención de descifrarlos una vez que la tecnología cuántica madure.

A diferencia del impacto disruptivo total de Shor sobre la criptografía asimétrica, el algoritmo de Grover proporciona una aceleración cuadrática en la búsqueda en bases de datos no estructuradas. En el contexto de la cadena de bloques, esto afecta principalmente a las funciones hash utilizadas para la minería (prueba de trabajo o PoW) y para la vinculación de bloques en el registro. Un ordenador cuántico podría encontrar colisiones de hash o invertir una función hash con un esfuerzo que reduce efectivamente la seguridad de los bits a la mitad. Por ejemplo, una función hash con 256 bits de seguridad frente a ataques clásicos solo proporcionaría 128 bits de seguridad frente a un ataque cuántico (véase la Tabla 1).

Tabla 1: El algoritmo de Grover y la degradación de la seguridad simétrica y las funciones hash

Algoritmo	**Propósito**	**Vulnerabilidad Cuántica**	**Impacto en la integridad**
RSA-2048	Firmas / Cifrado	Algoritmo de Shor	Ruptura total (Existencial)
ECDSA	Firmas digitales	Algoritmo de Shor	Ruptura total (Existencial)
SHA-256	Hash / Minería PoW	Algoritmo de Grover	Reducción a 128 bits (Manejable)
AES-256	Cifrado simétrico	Algoritmo de Grover	Reducción a 128 bits (Seguro)
SHA-384	Hash de alta seguridad	Algoritmo de Grover	Reducción a 192 bits (Seguro)

La implicación directa para la integridad de los datos es que un atacante

cuántico podría, en teoría, reescribir la historia de una cadena de bloques si posee suficiente ventaja computacional, alterando transacciones pasadas sin que el resto de la red pueda detectar la inconsistencia de inmediato, a menos que se aumenten los parámetros de seguridad.

Criptografía poscuántica: La transición hacia la resiliencia algorítmica

Ante la inminencia de la era cuántica, la comunidad internacional ha acelerado el desarrollo de la criptografía poscuántica (PQC), que se refiere a algoritmos criptográficos que se ejecutan en ordenadores clásicos pero que son resistentes a los ataques de ordenadores cuánticos. El Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos ha liderado un proceso de estandarización global que culminó en 2024 con la publicación de los primeros estándares finales: FIPS 203, FIPS 204 y FIPS 205.

Análisis de los esquemas de firma basados en redes (Lattices)

Los algoritmos basados en redes, como CRYSTALS-Dilithium (estandarizado como ML-DSA) y Falcon (FN-DSA), se fundamentan en la dificultad de encontrar el vector más corto en una red multidimensional, un problema que se considera resistente incluso para los ordenadores cuánticos más potentes. Estos algoritmos ofrecen un equilibrio entre el tamaño de la clave y la velocidad de procesamiento, lo cual es vital para los sistemas de cadena de bloques que requieren una validación de transacciones con baja latencia.

Sin embargo, la implementación de ML-DSA en las cadenas de bloques existentes plantea desafíos técnicos significativos. El tamaño de una firma digital clásica (ECDSA) es de aproximadamente 64 bytes, mientras que una firma ML-DSA-65 (Nivel 3 de seguridad) es de 3 bytes. bytes. Este aumento de casi 50 veces en el tamaño de los datos de transacción provocaría una degradación masiva del rendimiento de la red y un aumento exponencial de los requisitos de almacenamiento de los nodos.

Criptografía basada en hashes y su robustez

El estándar SPHINCS+ (SLH-DSA) representa un enfoque diferente que se basa únicamente en la seguridad de las funciones hash. Aunque es extremadamente robusto porque no depende de supuestos matemáticos complejos que podrían ser vulnerados por nuevos algoritmos cuánticos, sufre de firmas digitales masivas (cercanas a los 30 KB por firma en configuraciones seguras), lo que lo vuelve impracticable para la mayoría de las aplicaciones de cadena de bloques en su forma nativa (Magyari y Chen, 2025).

Para resolver este dilema de almacenamiento, se han propuesto arquitecturas híbridas. Una de las soluciones más prometedoras es la integración de la cadena de bloques con el Sistema de Archivos Interplanetario (IPFS). En este modelo, las claves públicas y las firmas poscuánticas de gran tamaño se almacenan en IPFS y solo el hash de referencia de 32 bytes se registra en la cadena de bloques. Este enfoque ha demostrado reducir el tamaño de los datos en la cadena en más del 99% para algoritmos como SPHINCS+, lo que permite mantener la integridad sin sacrificar la escalabilidad del sistema.

Impacto cuantitativo en las redes de Bitcoin y Ethereum

La migración a la criptografía poscuántica no es una simple actualización de software; es lo que los expertos denominan una degradación defensiva. Esto se debe a que la PQC impone costos inmediatos y severos en términos de capacidad de procesamiento y de almacenamiento sin ofrecer beneficios tangibles inmediatos para el usuario final, más allá de la protección contra una amenaza futura.

La investigación en sistemas permisionados como Hyperledger Fabric ha mostrado una degradación del rendimiento (*throughput*) del 52% al 57% al implementar firmas poscuánticas. En redes públicas y globales como Bitcoin o Ethereum, que operan en hardware heterogéneo y enfrentan latencias de propagación a nivel mundial, se estima que la pérdida de capacidad podría alcanzar entre el 60% y el 70% (véase la Tabla 2)

Tabla 2: Degradación del rendimiento y aumento de costos

Métrica de Impacto	**Estado Clásico (ECDSA)**	**Estado Post-Cuántico (ML-DSA-65)**	**Factor de Cambio**
Tamaño de salida UTXO (Bitcoin)	~22 bytes	~1,960 bytes	~89x aumento

Tamaño del conjunto UTXO total	~5 GB	~296 GB	~59x aumento
Estado permanente (Ethereum)	Base	+1 TB en 5 años	Crítico
Latencia de transacción	Base	+80-120%	~2x aumento
Tarifas de red (*Fees*)	Base	2x - 3x aumento	Económico

Este bloqueo de estado (state bloat) es una de las mayores preocupaciones para la integridad a largo plazo. Si los requisitos de almacenamiento para un nodo completo pasan de 1 TB a 10 TB, el número de participantes capaces de validar la red disminuirá, lo que llevará a una centralización forzada que, irónicamente, podría comprometer la integridad del sistema ante ataques convencionales del 51%.

Innovaciones en la integridad cuántica: cadenas de bloques nativas

Mientras que la criptografía poscuántica busca proteger los sistemas

clásicos, una nueva frontera de investigación propone la creación de cadenas de bloques intrínsecamente cuánticas. Estos sistemas no solo resisten ataques cuánticos, sino que también aprovechan las propiedades de la mecánica cuántica para garantizar una inmutabilidad superior.

Entrelazamiento temporal y el concepto de influencia no clásica sobre el pasado

Una propuesta conceptual disruptiva consiste en codificar la cadena de bloques en un estado Greenberger-Horne-Zeilinger (GHZ) temporal de fotones que no pueden coexistir simultáneamente. A diferencia del entrelazamiento espacial convencional, el entrelazamiento temporal vincula un bloque de datos actual con un estado cuántico ya medido y ya inexistente.

El proceso matemático puede describirse mediante la creación de estados de Bell temporales:

$$|\beta_{r_1 r_2}\rangle_{0,\tau} = \frac{1}{\sqrt{2}}(|0^0\rangle|r_2^\tau\rangle + (-1)^{r_1}|1^0\rangle|\bar{r}_2^\tau\rangle)$$

Donde $r_1 r_2$ representa el registro clásico de dos bits. Al concatenar estos estados, se forma una cadena en la que el presente está físicamente entrelazado con el pasado. Cualquier intento de alterar un bloque anterior destruiría de forma detectable e irreversible el entrelazamiento del bloque actual. Los investigadores sostienen que este diseño puede interpretarse como una forma de influir no clásicamente en el pasado, proporcionando una garantía de integridad que no depende de la computación, sino de la propia estructura del tiempo y de la materia.

El protocolo θ para la verificación distribuida

Para validar estos estados GHZ en una red distribuida, se utiliza el protocolo θ. En este esquema, un nodo verificador distribuye qubits individuales a cada nodo de la red. Cada nodo realiza una medición local basada en un ángulo θ_j asignado aleatoriamente. La integridad del bloque se confirma si la suma XOR de los resultados de las mediciones satisface la condición:

$$\bigoplus_j Y_j = \frac{1}{\pi} \sum_j \theta_j \pmod 2$$

Este protocolo permite que, incluso en presencia de nodos deshonestos, la red alcance un consenso sobre la autenticidad del estado cuántico del registro con una probabilidad cercana a 1.

Aplicación en sistemas complejos I: Salud y registros clínicos

La integridad de los datos en el sector salud es una cuestión de vida o muerte. La falsificación o alteración de registros clínicos puede llevar a diagnósticos erróneos, tratamientos inadecuados o fraudes masivos en ensayos clínicos. La combinación de la computación cuántica y la cadena de bloques ofrece una solución robusta para este entorno.

El ecosistema QUMA (Quantum Unified Medical

Architecture)

El marco QUMA propone un modelo de confianza multipartito diseñado para proteger los registros electrónicos de salud (EHR) frente a adversarios cuánticos. A diferencia de los sistemas tradicionales, QUMA utiliza BloQs (bloques cuánticos) que emplean qubits para almacenar los hashes de los bloques individuales.

Una de las innovaciones clave en QUMA es el uso de funciones hash cuánticas (QHF) basadas en caminatas cuánticas. Estos algoritmos han demostrado una sensibilidad estadística sin precedentes: una alteración de apenas el 0,25% en una cadena de datos clínicos provoca una variación del 35% o más en el valor del hash. Esta propiedad garantiza que cualquier manipulación, por mínima que sea, sea detectada de inmediato por la red.

Además, el protocolo EQHR (Entangled Quantum Health Record) facilita la distribución segura de claves mediante estados de Bell para autenticar a los usuarios del sistema. En situaciones críticas, como el intercambio de datos de tumores cerebrales o la gestión de la donación de órganos, la transparencia y la inmutabilidad de la cadena de bloques aseguran que la trazabilidad de la muestra o del órgano sea auditable y precisa, eliminando errores humanos y fraudes en la asignación.

Aplicación en sistemas complejos II: Cadenas de suministro inteligentes

Las cadenas de suministro modernas, especialmente en sectores como la construcción y la industria pesada, son ecosistemas opacos, con múltiples intermediarios y vulnerables a fraudes en materia de materiales y a retrasos administrativos.

Implementación del marco QBUILD

El sistema QBUILD es una arquitectura de cadena de bloques resistente a la computación cuántica diseñada para la transparencia en el suministro de la construcción. Basado en Hyperledger Fabric, integra las firmas digitales CRYSTALS-Dilithium y los mecanismos de intercambio de claves Kyber para asegurar la comunicación entre los nodos de la red.

En pruebas realizadas en entornos empresariales reales (como la multinacional SIL), el marco QBUILD demostró mejoras operativas notables:

1. **Resiliencia de seguridad:** Un aumento del 50% en la capacidad de resistir ataques simulados, incluidos los basados en Shor.
2. **Eficiencia de transacciones:** Una reducción del 40% en la latencia de las transacciones (de 5 a 3 segundos), facilitada por la optimización de los contratos inteligentes y el uso del protocolo de consenso Raft.
3. **Visibilidad y trazabilidad:** Una mejora del 35% en la eficiencia de seguimiento mediante el uso de sensores IoT protegidos por identidades cuánticas, con una precisión del 98% en el rastreo de activos.

Este nivel de integridad asegura que los pagos solo se liberen cuando se verifiquen automáticamente las condiciones de entrega de materiales, lo que reduce los retrasos en los pagos en un 47%, un problema histórico en la industria.

Aplicación en sistemas complejos III: Infraestructuras críticas y energía

La integridad de la red eléctrica es un pilar de la seguridad nacional. Con la transición hacia redes inteligentes y mercados energéticos distribuidos, la vulnerabilidad de las comunicaciones entre subestaciones y centros de control se ha convertido en un riesgo crítico.

Proyectos BLOSEM y KISS del PNNL

El Laboratorio Nacional del Pacífico Noroeste (PNNL) ha desarrollado dos iniciativas fundamentales para integrar la integridad de la cadena de bloques en la red eléctrica:

- **BLOSEM (Blockchain for Optimized Security and Energy Management):** Un marco de colaboración diseñado para estandarizar las métricas de seguridad de los dispositivos de red y las comunicaciones resilientes. Su objetivo es asegurar que cada dispositivo de la red eléctrica tenga una identidad inmutable registrada en un libro mayor distribuido.
- **KISS (Keyless Infrastructure Security Solutions):** Este proyecto utiliza una infraestructura de firma sin llave (KSI) para verificar en tiempo real la integridad de las transacciones de energía. Al integrar KSI con la

plataforma VOLTTRON (un software de control y detección distribuida), el PNNL ha demostrado la capacidad de asegurar tanto los datos en reposo en los historiadores de las empresas de servicios públicos como los datos en tránsito entre los centros de control y las subestaciones.

La aplicación de contratos inteligentes en este ámbito permite la verificación automática de miles de transacciones de energía distribuida (como el comercio de energía solar entre hogares) en tiempo real, garantizando que el balanceo de carga de la red se base en datos íntegros y no manipulados por atacantes externos.

Estrategias de migración y gobernanza estratégica

La transición hacia una integridad resistente a la cuántica no es un evento único, sino un proceso plurianual de gestión de riesgos que requiere una coordinación sin precedentes entre los sectores público y privado.

El Índice de Criticidad Cuántica (QCI)

La integridad de los datos no solo depende del software, sino también de la resiliencia de la cadena de suministro de hardware cuántico. El Índice de Criticidad Cuántica (QCI) es una herramienta de evaluación triaxial que permite a los responsables de políticas identificar vulnerabilidades en el suministro de materiales raros (como el helio-3 o el molibdeno) necesarios para la computación cuántica.

Este marco se complementa con la migración a la PQC, formando un modelo de doble pilar: mientras que la PQC protege la integridad de los datos digitales contra campañas de "cosechar ahora, descifrar después", el QCI asegura que la infraestructura física necesaria para la defensa cuántica sea estable y segura.

Las organizaciones deben adoptar un enfoque de priorización basado en niveles de migración:

- **Pequeñas empresas (5-7 años):** Enfoque en la actualización de software y en servicios en la nube con soporte PQC.
- **Medianas empresas (8-12 años):** requieren actualizaciones de la infraestructura interna y coordinación con proveedores clave.
- **Grandes empresas e infraestructuras críticas (12-15+ años):** Debido a la complejidad de los sistemas heredados (*legacy*) y a las dependencias regulatorias globales, estas organizaciones tienen el camino más largo hacia la resiliencia total (Norikane y Nishimura, 2025).

La convergencia entre la computación cuántica y la cadena de bloques representa la evolución definitiva de la integridad de los datos. Lo que comenzó como una vulnerabilidad existencial se ha transformado en una oportunidad para construir sistemas complejos cuya inmutabilidad no se basa únicamente en la dificultad matemática, sino en las leyes inviolables de la física cuántica.

La integridad de los datos en sistemas complejos requiere hoy una estrategia multidimensional que combine:

1. **Agilidad criptográfica:** La capacidad de los sistemas de cadena de

bloques para rotar algoritmos PQC (como ML-DSA y SPHINCS+) sin interrupciones operativas masivas (Magyari y Chen, 2025).

2. **Arquitecturas híbridas de almacenamiento:** El uso de IPFS y otras tecnologías de almacenamiento descentralizado para mitigar el impacto del tamaño de los datos poscuánticos.
3. **Seguridad física y de suministro:** El fortalecimiento de las cadenas de suministro de hardware mediante marcos como el QCI para garantizar que los sistemas de defensa cuántica puedan construirse y mantenerse.
4. **Innovación en protocolos cuánticos nativos:** La transición hacia registros entrelazados temporalmente que ofrezcan una integridad probada por el entrelazamiento cuántico, eliminando la posibilidad de manipulación retroactiva de forma absoluta (Dix et al., 2025).

A medida que nos acercamos al horizonte de los ordenadores cuánticos criptográficamente relevantes, la integridad de la información dejará de ser una preocupación técnica para convertirse en la base de la soberanía nacional y de la estabilidad de la civilización digital. El éxito de esta transición dependerá de una acción proactiva inmediata, reconociendo que la ventana de amenaza no es un problema del mañana, sino una realidad operativa del presente.

Capítulo 4

Estrategias de ciberseguridad avanzada para la detección de vulnerabilidades en tiempo real mediante modelos de confianza cero

El panorama contemporáneo de la seguridad digital ha experimentado una metamorfosis radical, impulsada por la disolución de los perímetros tradicionales, la migración masiva hacia entornos de nube híbrida, el trabajo remoto y la proliferación de dispositivos del Internet de las Cosas (IoT). En este contexto, el modelo convencional de castillo y foso, que prioriza la defensa de un perímetro estático, ha demostrado ser insuficiente frente a las amenazas sofisticadas y la movilidad de los activos modernos.

La arquitectura de Confianza Cero (Zero Trust Architecture o ZTA) emerge como el paradigma correctivo fundamental, basado en la premisa de que ninguna entidad, ya sea interna o externa, debe gozar de confianza implícita (Xu et al., 2005). Este informe analiza exhaustivamente los mecanismos de detección de vulnerabilidades en tiempo real, la integración de inteligencia artificial y la implementación de controles adaptativos que definen la ciberseguridad avanzada en la era de la transformación digital.

El Colapso del Modelo de Perímetro y la Génesis de Zero Trust

Históricamente, las organizaciones confiaban en la ubicación de la red como el principal indicador de seguridad. Una vez que un usuario o dispositivo superaba las defensas perimetrales, como firewalls o gateways, se le concedía un acceso excesivamente amplio a los recursos internos, lo que permitía a los atacantes moverse lateralmente con relativa libertad tras un compromiso inicial. El modelo Zero Trust, conceptualizado inicialmente por analistas de Forrester en 2010, propone un giro de 180 grados: nunca confiar, siempre verificar. Esta filosofía asume que la brecha de seguridad no es solo una posibilidad, sino una inevitabilidad, lo que obliga a los equipos de seguridad a diseñar controles capaces de contener amenazas que ya han eludido las defensas iniciales.

La evolución de este concepto ha estado cimentada en estándares internacionales, entre los que destaca la Publicación Especial 800-207 del Instituto Nacional de Estándares y Tecnología (NIST), que define la ZTA no como un producto único, sino como una estrategia holística centrada en la protección de recursos individuales. La transición hacia este modelo implica un cambio de la defensa de segmentos de red estáticos a la defensa activa de los usuarios, los activos y los datos, independientemente de su ubicación física o lógica (véase la Tabla 4).

Tabla 4: Comparación del modelo de perímetro y la génesis de zero trust

Dimensión de Seguridad	**Modelo Tradicional de Perímetro**	**Arquitectura Zero Trust (ZTA)**
Supuesto de confianza	Confianza implícita en la red.	Ninguna entidad es confiable por defecto.
Acceso a recursos	Con base en la ubicación de la red y en las credenciales estáticas.	Basado en la identidad, el contexto y el riesgo dinámico.
Movimiento Lateral	Facilitado por la falta de segmentación interna.	Mitigado mediante microsegmentación granular.
Verificación	Realizada una sola vez en el punto de entrada.	Continúa durante toda la sesión.
Visibilidad	Limitada a los puntos de entrada y salida de la red.	Total y en tiempo real mediante telemetría unificada.

Pilares Arquitectónicos del NIST SP 800-207

La implementación de una estrategia de Confianza Cero efectiva requiere una comprensión profunda de sus componentes lógicos y funcionales. El marco del NIST establece una separación estricta entre el plano de control y el plano de datos, garantizando que las decisiones de acceso se tomen de manera centralizada y se apliquen de forma distribuida (Abdelmagid y Diaz, 2025).

El Punto de Decisión de Políticas (PDP)

El PDP actúa como el cerebro del sistema, evaluando cada solicitud de acceso en función de múltiples señales. Se divide en dos subcomponentes críticos: el Motor de Políticas (Policy Engine, o PE) y el Administrador de Políticas (Policy Administrator, o PA). El PE utiliza un algoritmo de confianza que ingiere datos de diversas fuentes, entre ellas los sistemas de gestión de identidad (IAM), la telemetría de dispositivos (CDM), la inteligencia de amenazas y los logs de actividad. El PA, por su parte, es responsable de ejecutar la decisión del PE, generar las credenciales o tokens específicos para la sesión y comunicarlos al punto de ejecución (Janaćković et al., 2025).

El Punto de Ejecución de Políticas (PEP)

El PEP es el componente que intercepta y permite, monitoriza o termina las conexiones entre el sujeto y el recurso. Se despliega lo más cerca posible del recurso protegido, a menudo en forma de proxies de identidad, gateways de seguridad o agentes integrados en las cargas de trabajo. Una característica distintiva de los PEP modernos es su capacidad para establecer conexiones de adentro hacia afuera, lo que elimina la necesidad de direcciones IP públicas y protege las aplicaciones frente a escaneos oportunistas en internet.

Detección de Vulnerabilidades en Tiempo Real mediante Telemetría

La eficacia de Zero Trust para detectar vulnerabilidades en tiempo real radica en su capacidad para convertir la telemetría bruta en inteligencia accionable. A diferencia de los modelos reactivos que dependen de auditorías periódicas, la ZTA requiere visibilidad continua y granular de cada transacción.

Análisis de Comportamiento de Usuarios y Entidades (UEBA)

El UEBA representa una de las innovaciones más potentes en la detección de amenazas internas y de abusos de credenciales. Mediante el uso de aprendizaje automático (ML), el sistema establece una línea de base de comportamiento normal para cada usuario, dispositivo y servicio durante un periodo de aprendizaje de 60 a 90 días. Una vez establecida esta base, cualquier desviación significativa —como un acceso inusual a una base de datos a medianoche o la descarga de volúmenes atípicos de datos— activa una alerta inmediata o una reevaluación del riesgo en tiempo real.

Este enfoque es particularmente crucial porque el 80% de los ataques modernos no utilizan malware, sino que se basan en el uso de credenciales legítimas robadas. El UEBA permite identificar estas intrusiones al detectar inconsistencias de comportamiento que las herramientas basadas en reglas estáticas ignorarían. Por ejemplo, el fenómeno del viaje imposible (un acceso desde dos ubicaciones geográficamente distantes en un intervalo de tiempo físicamente imposible) es una señal clara de compromiso que el PDP puede

procesar para revocar de inmediato el acceso.

Monitorización de la Postura de Seguridad y Salud de los Dispositivos

En un ecosistema Zero Trust, la identidad no es el único factor decisorio; la salud del dispositivo es igualmente crítica. Las herramientas de gestión unificada de endpoints (UEM) y de detección y respuesta en endpoints (EDR) proporcionan señales constantes sobre el estado del hardware y el software. Si un dispositivo intenta acceder a un recurso crítico mientras su sistema operativo no está parcheado contra una vulnerabilidad de día cero conocida, o si el cifrado del disco está desactivado, el sistema puede denegar el acceso automáticamente (Xu et al., 2025). Esta evaluación continua de la postura garantiza que el riesgo se gestione de forma dinámica, adaptándose a las vulnerabilidades recién descubiertas al momento de solicitar acceso.

El rol de la inteligencia artificial y el aprendizaje automático

La escala y la velocidad de los ataques actuales superan la capacidad de respuesta de los analistas humanos, lo que convierte a la Inteligencia Artificial (IA) en un componente indispensable de la ZTA avanzada. La IA actúa como el tejido conectivo que permite orquestar y automatizar la seguridad a escala global.

Puntuación Dinámica de Riesgo

La IA permite que el PDP pase de decisiones binarias

(permitir/denegar) a una evaluación matizada mediante la puntuación dinámica de riesgo. Los modelos de IA procesan millones de eventos en tiempo real para asignar una puntuación numérica al riesgo asociado a una solicitud específica. Factores como la ubicación geográfica, la hora del día, el historial de comportamiento y la integridad del dispositivo se ponderan de forma instantánea. Si el riesgo supera un umbral predefinido, el sistema puede forzar automáticamente una autenticación multifactor (MFA) adicional, limitar el acceso a un subconjunto de datos o aislar la sesión por completo.

Detección Proactiva de Anomalías y Reducción del Tiempo de Dwell

La capacidad de la IA para identificar patrones invisibles al ojo humano le permite detectar vulnerabilidades en tiempo real antes de que sean explotadas. Los algoritmos de aprendizaje profundo (Deep Learning) pueden analizar el tráfico cifrado —donde se oculta más del 87% de las amenazas actuales— sin necesidad de descifrarlo por completo, buscando señales sutiles de exfiltración de datos o de comunicación con servidores de comando y control (Muller et al., 2023). Esto reduce drásticamente el tiempo de permanencia (dwell time) de un atacante en la red, que tradicionalmente promediaba 207 días en organizaciones sin seguridad impulsada por IA.

Microsegmentación: conteniendo el radio de explosión

Uno de los objetivos fundamentales de Zero Trust es minimizar el radio

de explosión (blast radius) de cualquier brecha. La segmentación de red tradicional, basada en subredes y VLANs, resulta demasiado tosca para detener los ataques modernos. La microsegmentación, en cambio, permite aislar cargas de trabajo, procesos y dispositivos individuales.

La Analogía de los Mamparos en la Ingeniería Naval

El papel de la microsegmentación se asemeja al de los mamparos en el casco de un barco. Si se produce una brecha, solo el compartimento afectado se inunda, lo que evita que toda la nave se hunda. De manera similar, si un servidor web es comprometido, la microsegmentación impide que el atacante se mueva hacia la base de datos o el sistema de facturación, ya que no existe una ruta de red permitida ni confianza implícita entre esos segmentos.

Acceso Controlado por Políticas y JIT (Just-In-Time)

La microsegmentación avanzada se implementa mediante políticas dinámicas que utilizan atributos de identidad en lugar de direcciones IP. El acceso Just-In-Time (JIT) permite que los privilegios elevados se otorguen solo cuando se necesitan y por un periodo estrictamente limitado. Esto elimina los privilegios permanentes, una de las vulnerabilidades más explotadas por los actores de amenazas para escalar privilegios y exfiltrar datos sensibles. El uso de microperímetros definidos por software garantiza que la seguridad sea intrínseca a la carga de trabajo, acompañándola incluso al migrar entre diferentes nubes o centros de datos.

Integración de Ecosistemas Unificados: SASE y XDR

Para lograr una detección de vulnerabilidades efectiva en tiempo real, las organizaciones están convergiendo sus herramientas en plataformas unificadas. El modelo SASE (Secure Access Service Edge) y la solución XDR (Extended Detection and Response) son los dos pilares de esta integración.

Secure Access Service Edge (SASE)

SASE unifica las capacidades de red (SD-WAN) con funciones de seguridad entregadas en la nube, como el acceso a la red Zero Trust (ZTNA), firewalls como servicio (FWaaS) y agentes de seguridad de acceso a la nube (CASB). Al consolidar estos servicios, SASE simplifica la gestión y garantiza que las políticas de Zero Trust se apliquen de manera uniforme a todos los usuarios, ya sea que estén en la oficina central, en una sucursal o trabajando desde una cafetería. La plataforma actúa como un conmutador inteligente que conecta a los usuarios directamente con las aplicaciones mediante una red global optimizada, eliminando el cuello de botella de las VPN tradicionales.

Extended Detection and Response (XDR)

Mientras que SASE se centra en el acceso seguro, XDR se enfoca en la visibilidad y la respuesta a lo largo de todas las capas de seguridad: endpoints, redes, nubes y correo electrónico. XDR ingiere telemetría de diversas fuentes y utiliza IA para correlacionar eventos que, de forma aislada, podrían parecer benignos, pero que, en conjunto, revelan un ataque complejo y coordinado.

Esta visibilidad holística es esencial para la detección de vulnerabilidades en tiempo real, ya que permite identificar vectores de ataque que atraviesan distintos silos tecnológicos.

Desafíos Técnicos y Compromisos de Rendimiento

A pesar de sus beneficios teóricos, la implementación de Zero Trust plantea desafíos operativos significativos que pueden afectar la eficiencia del negocio si no se gestionan adecuadamente.

La Tríada de Latencia, Rendimiento y Seguridad

La verificación continua introduce inherentemente una carga computacional. Cada solicitud de acceso requiere una consulta al PDP, una validación del estado del dispositivo y, posiblemente, la negociación de un túnel cifrado (como mTLS). En entornos de IoT industrial o de telemedicina, donde los tiempos de respuesta deben ser inferiores a 10 ms, la latencia introducida por los protocolos de seguridad estándar puede provocar inestabilidad en el sistema. Los datos empíricos indican que el cifrado y el aislamiento pueden implicar una sobrecarga de recursos de hasta el 12%, lo que obliga a las organizaciones a buscar marcos de Zero Trust ligeros que utilicen criptografía optimizada para dispositivos con recursos limitados.

El Reto de los Sistemas Legados

Muchos entornos corporativos dependen de aplicaciones diseñadas en

décadas pasadas que no admiten protocolos de autenticación modernos ni la segmentación granular. Integrar estos sistemas en una ZTA requiere estrategias creativas, como el uso de proxies de acceso que actúan como traductores de identidad o la creación de enclaves de red específicos que aíslan el sistema legado mediante firewalls de capa. Ignorar estos sistemas no es una opción, ya que a menudo constituyen los eslabones más débiles y las vulnerabilidades más críticas de la cadena de seguridad.

La implementación de múltiples puertas de verificación puede percibirse como una barrera para la productividad. Si los usuarios se ven obligados a realizar MFA constantemente para tareas triviales, la moral disminuirá y buscarán atajos para eludir los controles de seguridad. Por ello, las mejores prácticas sugieren un despliegue por fases, comenzando por los activos de mayor riesgo y utilizando la autenticación adaptativa para minimizar la fricción en las actividades de bajo riesgo (véase la Tabla 5).

Tabla 5: Gestión del cambio y experiencia del usuario

Desafío de Implementación	**Impacto en la Detección**	**Estrategia de mitigación**
Latencia de Red	Retraso en la validación de transacciones.	Uso de PEP distribuidos en el Edge.
Silos de Datos	Visibilidad fragmentada de	Implementación de lagos de

	vulnerabilidades.	datos de seguridad (SIEM/XDR).
Fricción del usuario	Intento eludir controles de seguridad.	SSO y MFA basados en el riesgo (Adaptive Auth).
Complejidad de Políticas	Riesgo de configuraciones erróneas.	Automatización y orquestación de políticas (IA).
Escalabilidad en IoT	Dificultad para gestionar miles de sensores.	Protocolos de comunicación ligeros y Zero-Touch.

Casos de Uso y Validación en el Mundo Real

La efectividad del modelo Zero Trust se ha validado en diversos sectores críticos, lo que demuestra que es posible equilibrar la seguridad avanzada con la continuidad operativa.

Transformación a Gran Escala: El Departamento de Defensa (DoD)

Tras el masivo compromiso de SolarWinds, el DoD de EE. EE. EE. EE. UU. lanzó una de las iniciativas de Zero Trust más ambiciosas del mundo, con una inversión específica de 977 millones de dólares para la transición inicial. El

objetivo es alcanzar un nivel de madurez avanzado para 2032, con enfoque en 91 resultados de capacidad medibles. El DoD ha demostrado que Zero Trust a escala requiere una transformación organizacional total, abordando la seguridad no como un gasto tecnológico, sino como un habilitador estratégico para las operaciones de defensa global.

Resiliencia en el Sector Salud: NHS y UVM Health

Los hospitales son objetivos prioritarios para el ransomware debido a la naturaleza crítica de sus datos y servicios. Organizaciones como BrisDoc y varios fideicomisos del NHS en el Reino Unido han reemplazado sus VPNs heredadas por plataformas de SASE Zero Trust. Esto ha permitido asegurar el trabajo híbrido de los clínicos y proteger los dispositivos médicos conectados sin interrumpir la atención al paciente (Lorenzoni et al., 2025). En incidentes reales de ransomware analizados, las organizaciones que habían implementado microsegmentación pudieron contener el ataque en un solo departamento, evitando el colapso sistémico que suele ocurrir en redes planas.

Productividad en la manufactura: el modelo alemán

Un fabricante alemán de tamaño medio adoptó el modelo Zero Trust como parte de su transformación hacia la Industria 4.0. Al eliminar las VPNs complejas y adoptar el acceso basado en la identidad, logró reducir el tiempo de incorporación de los proveedores de 3 semanas a solo 1 día. Además, la visibilidad total de los sistemas de tecnología operativa (OT) permitió detectar vulnerabilidades en tiempo real en la cadena de producción sin interrumpir los procesos industriales (Román et al., 2024).

El Futuro: Criptografía Post-Cuántica y Seguridad Autónoma

A medida que nos acercamos a la era de la computación cuántica, el modelo Zero Trust debe evolucionar para enfrentar amenazas que aún no existen de forma generalizada, pero que ya se están gestando.

La Amenaza Cuántica y el Ataque HNDL

Los ordenadores cuánticos suficientemente potentes podrán romper los algoritmos de cifrado asimétrico actuales (como RSA y ECC) mediante el algoritmo de Shor. Los actores de amenazas ya están practicando el Harvest Now, Decrypt Later (Recopilar ahora, descifrar después), robando hoy datos cifrados para descifrarlos cuando la tecnología cuántica madure en la próxima década.

La integración de la criptografía poscuántica (PQC) en el marco de Zero Trust es esencial para garantizar la confidencialidad a largo plazo. Las nuevas normas del NIST para algoritmos resistentes a ataques cuánticos deben integrarse en los procesos de autenticación y cifrado de las ZTA para que los túneles de comunicación y los depósitos de datos permanezcan seguros frente a futuros adversarios (Kang et al., 2023).

Hacia un ecosistema de seguridad autónomo

El futuro de la detección de vulnerabilidades en tiempo real apunta a sistemas autosanables. Impulsados por IA de nueva generación, estos ecosistemas no solo detectarán anomalías, sino que también ajustarán

dinámicamente las microsegmentaciones, revocarán automáticamente privilegios excesivos y parchearán vulnerabilidades críticas en el código en tiempo de ejecución, todo ello con una intervención humana mínima. Esta capacidad de respuesta a la velocidad de la máquina será la única defensa viable contra los ataques automatizados impulsados por la propia IA de los ciberdelincuentes.

La ciberseguridad avanzada para la detección de vulnerabilidades en tiempo real ya no puede depender de perímetros estáticos ni de verificaciones puntuales. El modelo Zero Trust ofrece la arquitectura necesaria para enfrentar un panorama de amenazas hiperdinámico, transformando la seguridad de un obstáculo operativo en un habilitador de confianza y resiliencia (Salem et al., 2024).

La clave para una implementación exitosa reside en la integración profunda de la telemetría, el uso estratégico de la IA para la toma de decisiones y la adopción de una mentalidad de asunción de brecha. Aunque los desafíos de latencia y la complejidad de los sistemas legados son reales, los beneficios en términos de reducción del riesgo, cumplimiento normativo y agilidad empresarial superan con creces los costes de la transición.

En última instancia, Zero Trust no es un destino final, sino un viaje continuo de adaptación y mejora. Las organizaciones que logren orquestar sus identidades, dispositivos y datos bajo este paradigma no solo estarán mejor protegidas contra los ataques actuales, sino que también habrán construido la base necesaria para prosperar en la era futura de la computación cuántica y la inteligencia artificial autónoma (Kang et al., 2023).

Capítulo 5

El ecosistema de los gemelos digitales: simulación avanzada y mantenimiento predictivo en la era de la industria 4.0 y 5.0

La evolución tecnológica contemporánea ha propiciado la aparición de paradigmas que fusionan indisolublemente el mundo físico y el digital. En el epicentro de esta transformación se encuentran los gemelos digitales, definidos como representaciones virtuales precisas de objetos, procesos o sistemas físicos que utilizan datos dinámicos para simular, analizar, supervisar y optimizar el rendimiento en tiempo real.

A diferencia de los modelos de simulación estáticos tradicionales, un gemelo digital se caracteriza por una conexión bidireccional y continua con su homólogo físico, lo que permite una convergencia de estados que evoluciona a lo largo de todo el ciclo de vida del activo, desde la fase inicial de diseño hasta su eventual desmantelamiento. Este fenómeno no constituye meramente una herramienta de visualización; representa una infraestructura crítica de conocimiento que permite a las organizaciones prever fallos, reducir costes operativos y acelerar la innovación mediante la experimentación en entornos virtuales seguros y de bajo riesgo (Salem et al., 2024).

Trayectoria del mercado global y dinámicas de adopción sectorial

El panorama económico de los gemelos digitales refleja un crecimiento exponencial impulsado por la maduración de tecnologías habilitadoras como el Internet de las Cosas (IoT), la computación en la nube y la inteligencia artificial (IA), que experimentó una tasa de crecimiento anual compuesta (CAGR) del 39,8%. Esta aceleración se sustenta en el reconocimiento, por parte de los líderes tecnológicos, del valor estratégico de estas réplicas; aproximadamente el 70% de los ejecutivos de corporaciones de gran escala ya destinan recursos específicos a iniciativas de gemelos digitales (Comisión Económica para América Latina y el Caribe, 2021).

La motivación detrás de estas inversiones ha trascendido la eficiencia puramente operativa para integrar objetivos de sostenibilidad y de gobernanza ambiental, social y corporativa (ESG). El 57% de las organizaciones identifican la sostenibilidad como un motor principal y utilizan gemelos digitales para monitorizar la huella de carbono y optimizar el consumo energético en tiempo real (véase la Tabla 6).

Tabla 6: Proyecciones y estadísticas de crecimiento del mercado de gemelos digitales

Métrica de Mercado	**Valor Estimado**	**Valor Proyectado**	**Fuente de Datos**
Mercado Global (Euros)	€16. mil millones	€242. mil millones	Fortune Business Insights
Tasa de crecimiento (CAGR)	39.%	39.%	Fortune Business Insights
Adopción en Grandes Corporaciones	70%	N/A	McKinsey
Planes de Integración para 2028	59%	N/A	ResearchAndMarkets.com
Crecimiento promedio de despliegue	36% (5 años)	N/A	Capgemini

El análisis de estos datos sugiere que la industria está abandonando los modelos de mantenimiento reactivos en favor de estrategias basadas en la condición real y en la predicción. Sectores como el aeroespacial, la construcción y la energía lideran esta transición, buscando no solo mitigar el tiempo de inactividad no planificado, sino también mejorar la resiliencia ante situaciones impredecibles mediante el uso de espacios de simulación seguros

(Norikane y Nishimura, 2025).

Arquitectura técnica y capas funcionales del Gemelo Digital

La eficacia de un gemelo digital depende de una orquestación compleja de capas tecnológicas que garantizan la integridad y la sincronización de los datos. La arquitectura puede desglosarse en componentes que abarcan desde el hardware sensorial hasta los motores de visualización avanzados.

Capa de activos físicos y adquisición de datos

En el nivel más elemental se encuentra el activo físico, que puede ser cualquier objeto, proceso o sistema real que se desee monitorizar. Este activo está equipado con una red de sensores IoT que capturan métricas críticas como la temperatura, la presión, la vibración y el flujo de energía. En el contexto de la Industria 4.0, a menudo se emplean objetos inteligentes con sensores preinstalados capaces de compartir datos de forma continua (Román et al., 2024). La transmisión de estos datos se realiza mediante tuberías de datos (data pipelines) que garantizan la sincronización en tiempo real entre el mundo físico y el virtual.

Modelado virtual y motores de simulación

El modelo virtual es la réplica digital construida a partir de los datos recopilados. Este modelo no es una imagen estática, sino que está embebido de atributos físicos y de leyes matemáticas que le permiten reaccionar de manera realista ante variables ambientales. Por ejemplo, el gemelo digital de

la turbina de un avión no solo refleja el estado actual, sino que también simula el desgaste aerodinámico y las fuerzas hidráulicas durante el vuelo. Los motores de análisis, a menudo potenciados por inteligencia artificial, procesan esta información para detectar anomalías y realizar predicciones.

Bucle de retroalimentación e integración de sistemas

Una característica definitoria del gemelo digital es el flujo bidireccional de información. Los conocimientos generados en el entorno virtual se devuelven al activo físico para optimizar su comportamiento, ya sea mediante ajustes automáticos o mediante decisiones humanas informadas. Esta integración se extiende a sistemas empresariales como el planeamiento de recursos empresariales (ERP) y la gestión de relaciones con clientes (CRM), lo que permite que las decisiones operativas estén alineadas con los objetivos de negocio y con la demanda del mercado.

Niveles de sofisticación y madurez tecnológica

No todos los gemelos digitales poseen las mismas capacidades analíticas. La industria reconoce una escala de sofisticación que clasifica los modelos según su nivel de autonomía y de procesamiento de datos. La transición del nivel descriptivo al nivel autónomo representa el camino hacia la Industria 5.0, en la que la colaboración entre humanos y sistemas inteligentes se vuelve más estrecha y proactiva. Actualmente, los sectores de arquitectura y construcción operan predominantemente en los niveles 1 y 2, mientras que la manufactura avanzada y la energía están empujando las fronteras hacia los niveles 3 y superiores.

Algoritmos de predicción de fallos y mantenimiento predictivo

El mantenimiento predictivo es quizás la aplicación más valiosa de los gemelos digitales en el ámbito industrial. Su objetivo es identificar el riesgo de fallo de un equipo antes de que ocurra una avería catastrófica, lo que permite programar reparaciones basadas en la necesidad real en lugar de en intervalos fijos.

Metodologías de inteligencia artificial y física informada

El núcleo de estas capacidades predictivas reside en la combinación del aprendizaje automático (Machine Learning) y el modelado basado en la física. Las Redes Neuronales Informadas por la Física (PINN, Physics-Informed Neural Networks) integran leyes físicas fundamentales, como la termodinámica o la mecánica de fluidos, en el proceso de entrenamiento de la red neuronal (Muller et al., 2023). Este enfoque híbrido permite una mayor precisión y capacidad de generalización, especialmente en situaciones en las que los datos de los sensores son ruidosos o incompletos.

Para el cálculo de la Vida Útil Remanente (RUL, Remaining Useful Life), se emplean arquitecturas de aprendizaje profundo como las Redes de Memoria a Largo Corto Plazo (LSTM, Long Short-Term Memory), que son excepcionalmente eficaces para analizar series temporales de datos de sensores y reconocer patrones de degradación.

La formalización matemática de este proceso de predicción se puede

expresar mediante una función de pérdida $\mathcal{L}$ que minimiza la diferencia entre el estado futuro predicho $\hat{\mathbf{x}}_{t+T}$ y el estado real $\mathbf{x}_{t+T}$:

$$\mathcal{L} = \mathbb{E}$$

Donde el estado predicho se obtiene mediante la función $\mathcal{F}$ aplicada a los datos históricos $\mathbf{X}_t$ y al horizonte temporal T:

$$\hat{\mathbf{x}}_{t+T} = \mathcal{F}(\mathbf{X}_t, T)$$

Este marco permite no solo predecir el fallo, sino también simular diferentes estrategias de intervención para seleccionar la que minimice el coste y el tiempo de inactividad.

Implementaciones en sectores estratégicos: casos de estudio

La adopción de gemelos digitales varía significativamente según la industria, adaptándose a los desafíos específicos de cada entorno operativo.

Aeroespacial y defensa

En el sector aeroespacial, los gemelos digitales se utilizan desde el diseño de aeronaves experimentales hasta el mantenimiento de motores en servicio. Boeing y la NASA son pioneros en el uso de réplicas virtuales para simular misiones espaciales y probar secuencias de comandos antes de enviarlas a las naves espaciales. Estas simulaciones permiten evaluar el

desgaste de componentes críticos bajo condiciones extremas de vibración y temperatura, lo que mejora la seguridad de los astronautas y la tasa de éxito de las misiones.

Energía y recursos naturales

La industria del petróleo y el gas utiliza gemelos digitales para obtener una visión dinámica de infraestructuras críticas como plataformas de perforación y refinerías. Mediante el uso de sensores IoT y analítica avanzada, los operadores pueden monitorizar la integridad de los oleoductos y optimizar la producción en tiempo real. En el ámbito de las energías renovables, los parques eólicos emplean gemelos de turbinas para ajustar el ángulo de las palas en función de los patrones de viento detectados, lo que aumenta la producción anual de energía (AEP) en varios puntos porcentuales.

Construcción y gestión de edificios

Los gemelos digitales están transformando la planificación urbana y la gestión de instalaciones al integrar modelos BIM (Building Information Modeling) con datos operativos en tiempo real. En los Estados Unidos, los edificios representan más del 30% de las emisiones de gases de efecto invernadero; el uso de gemelos digitales permite optimizar los sistemas de climatización (HVAC) y la iluminación, reduciendo las emisiones de carbono hasta en un 50%. Proyectos como el gemelo digital de Madrid utilizan modelos 3D/5D para representar las instalaciones municipales, lo que facilita la interoperabilidad entre organismos y mejora la gobernanza urbana.

Sector salud y biotecnología

En el ámbito de la salud, la tecnología se aplica tanto a nivel macro (gestión hospitalaria) como a nivel micro (modelado de órganos humanos). El uso de gemelos digitales de centros de salud permite simular el flujo de pacientes y la asignación de recursos, lo que reduce los tiempos de espera y optimiza los horarios de cirugía.

Un caso ejemplar es el desarrollo de gemelos digitales cardíacos que, a partir de datos de resonancia magnética (MRI) y electrocardiogramas (ECG), permiten a los cirujanos simular la respuesta de un paciente a diferentes tratamientos antes de realizar una intervención quirúrgica. Se estima que el 66% de los ejecutivos de salud prevén aumentar su inversión en estas tecnologías en los próximos años (Usländer et al., 2022).

Gemelo Digital de la Organización (DTO) y gestión estratégica

La extensión del concepto de gemelo digital a la estructura operativa de una empresa se denomina gemelo digital de la organización (DTO). A diferencia de los gemelos de activos individuales, un DTO representa los procesos de negocio, los sistemas y las interacciones humanas dentro de una organización.

Funcionalidades del DTO en la toma de decisiones

El DTO se alimenta de datos provenientes de sistemas operativos como ERP y CRM para garantizar una transparencia absoluta en el funcionamiento

de la empresa. Esto permite realizar simulaciones de cambios estructurales, como la introducción de una nueva línea de productos o la reestructuración de la cadena de suministro, para evaluar el impacto en los indicadores clave de rendimiento (KPI) antes de implementarlos en la práctica.

El uso de un DTO facilita la identificación de cuellos de botella en los flujos de trabajo y permite una gestión proactiva de los riesgos y del cumplimiento normativo. Al proporcionar un único punto de verdad para todos los interesados, el DTO mejora la alineación estratégica y reduce la incertidumbre asociada a las grandes transformaciones digitales.

Ecosistema de software y plataformas líderes

El mercado actual ofrece una diversidad de soluciones de software que se dividen en plataformas integrales de gestión de datos y en motores de simulación especializados.

La elección de una plataforma depende de factores como la disponibilidad de datos, la precisión requerida y los recursos computacionales. Mientras que Azure Digital Twins destaca por su capacidad para modelar relaciones complejas entre miles de activos, Siemens Xcelerator es preferido por los ingenieros que requieren una precisión física extrema en el diseño de productos (Krejčí et al., 2025). Un desarrollo significativo reciente es la alianza entre Siemens y NVIDIA para integrar Omniverse en el entorno Xcelerator, lo que permite visualizaciones inmersivas del Industrial Metaverse.

Estandarización, interoperabilidad y retos de implementación

A medida que las organizaciones despliegan múltiples gemelos digitales, surge la necesidad de que estos sistemas se comuniquen entre sí de manera eficiente. La interoperabilidad se ha identificado como el mayor reto técnico para la adopción a gran escala.

El marco de interoperabilidad ISO/IEC 30173

La norma internacional ISO/IEC 30173 busca unificar las definiciones y formalizar los conceptos clave del gemelo digital. Define al gemelo como una representación digital con conexiones de datos que permiten la convergencia entre los estados físico y digital a una tasa de sincronización adecuada. Este estándar es fundamental para evitar la creación de silos de información y permitir que gemelos de distintos proveedores interactúen en un ecosistema integrado.

Desafíos de ciberseguridad y gobernanza de datos

La digitalización de infraestructuras críticas mediante gemelos digitales amplía la superficie de ataque para los ciberdelincuentes. La protección de datos sensibles, como los diseños de productos y los parámetros operativos, es primordial. Las organizaciones deben implementar estrategias de seguridad avanzadas, como el cifrado de datos, la autenticación multifactor y la segmentación de redes, para cumplir con los protocolos industriales, como el estándar IEC 62443.

Además, la calidad de los datos es un factor crítico; si los datos de entrada son incompletos o erróneos, las simulaciones producirán resultados poco fiables (fenómeno conocido como garbage in, garbage out). Esto subraya la importancia de establecer una gobernanza de datos sólida con roles y estándares claros para el mantenimiento del modelo virtual.

Perspectivas futuras: Gemelos Digitales Cognitivos e Inteligencia Artificial Generativa

El futuro de la tecnología apunta a gemelos digitales cada vez más inteligentes y autónomos. Los Gemelos Digitales Cognitivos integran capacidades de computación cognitiva para aprender de la realidad, adaptarse dinámicamente y anticipar cambios futuros de manera similar a los procesos mentales humanos.

El impacto de los modelos fundacionales

La integración de modelos fundacionales de IA y de grandes modelos de lenguaje (LLM) permitirá que los gemelos digitales se conviertan en entidades proactivas capaces de razonar y generar escenarios creativos de forma autónoma (Armada et al., 2026). Estos sistemas podrán actuar como agentes inteligentes que optimizan operaciones en tiempo real sin intervención humana constante, marcando el comienzo de una era de gestión industrial verdaderamente autónoma.

En el ámbito de la ciencia básica, los gemelos digitales están acelerando el descubrimiento de nuevos materiales y el desarrollo de fármacos mediante

el uso de computación de alto rendimiento (HPC) y simulaciones de dinámica de fluidos a una escala antes inalcanzable (Hasan y Crawford, 2025). Iniciativas globales como el gemelo digital de la Tierra buscan modelar sistemas climáticos complejos para guiar las políticas de mitigación del cambio climático, lo que demuestra que el alcance de esta tecnología trasciende la industria para abordar los desafíos más urgentes de la humanidad.

Los gemelos digitales han dejado de ser una promesa tecnológica para convertirse en el pilar fundamental de la eficiencia y la resiliencia organizacionales en el siglo XXI. Su capacidad para integrar de forma dinámica el mundo físico y el virtual permite una optimización sin precedentes, garantizando que la toma de decisiones se base en evidencias, predicciones precisas y una comprensión profunda de la complejidad operativa (Armada et al., 2026; Inga, 2019).

Capítulo 6
Realidad virtual y aumentada: impacto en la industria y el diseño de interfaces

La convergencia tecnológica que define el panorama actual ha consolidado la realidad extendida (XR) y la computación espacial no solo como herramientas de visualización, sino también como infraestructura fundamental para la interacción humana con los datos y el entorno físico. Este cambio de paradigma representa una transición del uso de interfaces bidimensionales a la inmersión en ecosistemas digitales tridimensionales, donde el mundo real y el contenido generado por computadora coexisten indistintamente.

La evolución de estas tecnologías ha sido impulsada por una simbiosis entre hardware de alta fidelidad, redes de baja latencia como el 5G y el 6G, y una inteligencia artificial que actúa como el sistema operativo de la realidad misma. En este contexto, la aplicación de experiencias inmersivas abarca desde la capacitación técnica en entornos de alto riesgo hasta la redefinición absoluta de los principios de diseño de interfaces, priorizando la adaptabilidad contextual y la resonancia emocional del usuario (véase la Tabla 7).

Fundamentos conceptuales: de la realidad extendida a la computación espacial

Es imperativo establecer una distinción precisa entre la realidad extendida y la computación espacial. Mientras que la realidad extendida (XR) funciona como un término paraguas que agrupa a la realidad virtual (RV), la realidad aumentada (RA) y la realidad mixta (RM), la computación espacial es la disciplina que permite a las máquinas procesar y comprender el mundo físico para integrar lo digital de forma inteligente (Pérez et al., 2024) . Esta distinción no es meramente semántica; la computación espacial se centra en la capacidad de los sensores y algoritmos para detectar la posición, el movimiento y las interacciones en un espacio tridimensional, lo que permite que un modelo digital, por ejemplo, reconozca una superficie física y rebotar contra ella de manera realista.

La realidad virtual (RV) ha evolucionado para ofrecer experiencias de inmersión total, desconectando al usuario del entorno físico y transportándolo a escenarios simulados en los que la fidelidad visual y sonora es prácticamente idéntica a la de la realidad. Por otro lado, la realidad aumentada (RA) ha superado la fase de simples superposiciones para convertirse en una capa informativa persistente que enriquece la percepción del mundo real sin sustituirlo, apoyándose en dispositivos que van desde teléfonos inteligentes hasta gafas inteligentes ligeras y potentes (Martín et al., 2025).

La realidad mixta (RM) se sitúa en el punto de convergencia, permitiendo que los objetos digitales no solo coexistan con el mundo físico,

sino que interactúen con él, como un operario que visualiza instrucciones digitales ancladas directamente a la maquinaria que está reparando.

Tabla 7: Taxonomía de las tecnologías inmersivas

Concepto	**Definición Operativa**	**Interacción con el mundo físico**
Realidad extendida (XR)	Término general que engloba VR, AR y MR.	Variable según la tecnología específica.
Computación Espacial	Procesamiento de datos físicos para la integración digital.	Alta: requiere comprensión semántica del entorno.
Realidad virtual (RV)	Entorno simulado que reemplaza la visión del mundo real.	Nula: el usuario se abstrae del entorno físico.
Realidad aumentada (RA)	Superposición de datos digitales sobre la visión real.	Media: los datos se superponen, pero no interactúan entre sí.
Realidad Mixta (RM)	Híbrido en el que lo virtual	Máxima: los objetos digitales

	y lo físico interactúan en tiempo real.	obedecen a las leyes físicas.

La integración de la inteligencia artificial (IA) y el aprendizaje automático (ML) ha dotado a estos sistemas de capacidades predictivas y de reconocimiento de patrones en tiempo real. La IA será responsable de la interpretación de gestos complejos, del seguimiento ocular y de la comprensión del entorno, lo que permitirá que las interfaces inmersivas sean intuitivas y, en muchos casos, no requieran controladores físicos tradicionales (Ipuz et al., 2025). El uso de la computación en la nube y la computación de borde (edge computing) ha permitido delegar el procesamiento intensivo fuera de los dispositivos, lo que facilita el diseño de hardware más ergonómico y ligero sin sacrificar la potencia computacional necesaria para renderizar entornos fotorrealistas a 90 o 120 cuadros por segundo.

Transformación de la capacitación técnica y la formación profesional

El impacto más profundo de la realidad virtual se observa en la capacitación técnica y en la formación en seguridad industrial. La capacidad de replicar escenarios de alto riesgo en un entorno controlado ha transformado la pedagogía corporativa, permitiendo que los trabajadores practiquen habilidades críticas sin exponerse a peligros físicos ni incurrir en costos por daños a equipos reales (Llanos et al., 2025). Las organizaciones han

pasado de modelos de aprendizaje pasivos, basados en vídeos y presentaciones, a modelos experienciales en los que el error es una herramienta de aprendizaje segura.

Beneficios cuantitativos de la simulación inmersiva

Los datos confirman que la formación mediante RV es significativamente más efectiva que los métodos tradicionales. Los niveles de retención de conocimientos alcanzan hasta el 80% después de un año de la capacitación, en comparación con el escaso 5-10% obtenido con métodos convencionales. Esta efectividad se debe a la conexión emocional que genera la inmersión; los estudiantes se sienten 3,75 veces más vinculados emocionalmente con el contenido en RV que en un aula tradicional.

Casos de aplicación en seguridad y mantenimiento industrial

La empresa 3M ha desarrollado aplicaciones de RV para la seguridad en el trabajo, como la inspección de arneses de protección contra caídas y la demostración de soldadura, que permiten a los empleados experimentar las consecuencias de un equipo defectuoso o de una técnica incorrecta sin riesgo alguno. Estas simulaciones gamificadas aumentan el compromiso del trabajador y aseguran que los procedimientos se conviertan en respuestas instintivas. Las ventajas operativas de este enfoque son múltiples:

- Familiarización con los sitios remotos o peligrosos antes de la llegada física.
- Práctica de respuestas ante emergencias como incendios, fugas de gas o

derrames químicos.

- Estandarización de la calidad del entrenamiento en múltiples ubicaciones geográficas.
- Evaluación en tiempo real del desempeño del trabajador, identificando brechas en habilidades específicas mediante el análisis de datos de interacción.

Innovación en la medicina y los servicios de salud

La medicina ha adoptado la realidad virtual como un pilar fundamental tanto para la formación quirúrgica como para el tratamiento terapéutico. Las simulaciones médicas fotorrealistas permiten a los profesionales practicar cirugías complejas, realizar diagnósticos de trauma y responder ante desastres en entornos que imitan fielmente la presión y los desafíos de un quirófano real (Lorenzoni et al., 2025). El uso de estas tecnologías ha demostrado una reducción del 40% de los errores cometidos por cirujanos durante procedimientos reales, lo que subraya la importancia de la memoria muscular y de la toma de decisiones entrenadas en el mundo virtual.

Aplicaciones clínicas y terapéuticas de la RV

1. **Educación Quirúrgica y Procedimental**: Permite la práctica repetida de pasos quirúrgicos complejos, mejorando la precisión técnica y la confianza del cirujano antes de intervenir a un paciente.
2. **Formación en Enfermería y Cuidados Críticos**: Desarrolla habilidades clínicas y de toma de decisiones en el cuidado del paciente, simulando

situaciones de emergencia como paros cardiorrespiratorios.

3. **Salud Mental y Terapia Cognitiva**: La RV se utiliza para tratar el trastorno de estrés postraumático (TEPT), la ansiedad, el TDAH e incluso la ideación suicida mediante terapias de exposición controlada.
4. **Manejo de Equipos Médicos**: Capacitación en el uso y la resolución de problemas de dispositivos clínicos sofisticados, como máquinas de diálisis o ventiladores mecánicos, sin comprometer la integridad de los equipos costosos.
5. **Comunicación y Empatía**: Simulaciones diseñadas para fortalecer el trabajo en equipo y la interacción con el paciente, permitiendo a los profesionales practicar la comunicación de noticias difíciles o el manejo de situaciones conflictivas.

El mercado de la realidad virtual en la salud se proyecta en $11,3 mil millones para 2030, con una tasa de adopción superior al 30% en las escuelas de medicina de economías avanzadas. La accesibilidad global que ofrece la RV permite que especialistas de diferentes partes del mundo colaboren en la misma simulación, democratizando el acceso a conocimientos expertos y técnicas de vanguardia.

El diseño de interfaces (UI/UX) en la era tridimensional

El diseño de interfaces de usuario ha experimentado su transformación más radical desde la invención del ratón y el teclado. El diseño ya no se limita a pantallas planas; se ha expandido al espacio tridimensional, donde la

profundidad, la iluminación ambiental y la respuesta táctil son componentes críticos de la experiencia del usuario. Este nuevo enfoque, denominado diseño de interfaces espaciales, requiere que los diseñadores piensen en términos de volumen y distancia, tratando los elementos digitales como objetos con presencia física.

Tendencias dominantes en el diseño de interfaces

- **Liquid Glass y Glassmorphism**: Estas estéticas utilizan la transparencia, la refracción y el desenfoque para que los elementos digitales parezcan estar hechos de un material físico ligero. Los objetos reaccionan a la luz de la habitación y proyectan sombras dinámicas, lo que ayuda a integrar de forma natural el contenido virtual en el entorno real del usuario (Cipresso et al., 2018).
- **Interfaces Adaptativas e Hiperpersonalizadas**: Gracias a la IA, la interfaz cambia en tiempo real según el comportamiento del usuario, su estado emocional o su contexto inmediato. Si el sistema detecta señales de estrés o fatiga, puede simplificar los menús, atenuar los colores y reducir la velocidad de las animaciones para disminuir la carga cognitiva.
- **Interacciones Multimodales**: El usuario interactúa mediante una combinación de voz, gestos naturales (como señalar o pellizcar el aire), seguimiento ocular y retroalimentación háptica avanzada. El sistema puede predecir la intención del usuario simplemente analizando hacia dónde mira y la cadencia de sus gestos.
- **Microinteracciones Emocionales**: Las interfaces ya no solo responden de forma funcional, sino también de forma emocional. Una acción exitosa puede desencadenar una animación sutil y placentera (confeti digital o

un brillo cálido), mientras que un error puede manifestarse como una vibración suave o un gesto de rechazo de la interfaz, lo que humaniza la interacción tecnológica.

- **Diseño Phygital (Físico + Digital)**: La información digital se ancla de forma persistente a objetos físicos. Por ejemplo, al mirar un termostato real, las opciones de control digital aparecen flotando a su alrededor, lo que permite una interacción directa con dispositivos del Internet de las Cosas (IoT) mediante una capa de RA.

La reducción de la carga cognitiva es la máxima prioridad. Los diseñadores están abandonando la complejidad excesiva por interfaces minimalistas que solo muestran lo relevante en el momento preciso (UI ambiental), evitando abrumar al usuario con información innecesaria en su campo de visión.

Inteligencia artificial generativa y la creación de activos 3D

El despliegue masivo de experiencias inmersivas ha sido posible gracias a la maduración de la IA generativa, capaz de crear mundos y objetos tridimensionales. Los flujos de trabajo de diseño han pasado de meses de modelado manual a minutos de generación asistida por IA, democratizando la creación de contenido para pequeñas empresas y creadores individuales.

Estas herramientas no solo generan la geometría de los objetos, sino que también aplican texturas realistas y comportamientos físicos consistentes. Modelos avanzados como Genie 3 de Google pueden generar entornos

navegables completos en los que los personajes y objetos responden a las leyes de la física y a las acciones del usuario en tiempo real. Esta capacidad de bosquejar mundos con lenguaje natural permite que arquitectos, educadores e ingenieros visualicen conceptos complejos de forma instantánea, lo que acelera los ciclos de innovación.

Implementación regional y casos de éxito en el sector minero de Perú

Perú se ha posicionado como un referente regional en la adopción de tecnologías inmersivas aplicadas a la minería y la educación técnica. La industria minera peruana, motor de la economía nacional, ha integrado la RV y la RA para optimizar la seguridad, el mantenimiento y la formación de su fuerza laboral.

Transformación digital en las grandes operaciones mineras

- **Quellaveco (Anglo American)**: Es reconocida como la primera mina 100% digital del Perú. Utiliza una flota de camiones autónomos y gemelos digitales para monitorear en tiempo real las operaciones. La capacitación del personal incluye simulaciones avanzadas de RV para la inducción en seguridad y en la operación de equipos críticos, lo que contribuye a una cultura de trabajo proactiva y segura desde el inicio de sus operaciones (Usländer et al., 2022).
- **Cerro Verde y Antamina** han realizado inversiones significativas en equipamiento tecnológico y en simuladores de alta fidelidad para la formación de técnicos en mantenimiento preventivo y en protocolos de

seguridad industrial. Cerro Verde, en particular, ha reafirmado su compromiso con la minería responsable mediante una inversión de más de $300 millones orientada a la sostenibilidad y la innovación tecnológica.

- **Southern Peru Copper Corporation**: lidera las inversiones en el rubro de equipamiento minero tecnológico, integrando soluciones digitales que permiten una gestión más eficiente de los activos y una reducción de los riesgos operativos.

Factores humanos: ergonomía, salud y cinetosis (cybersickness)

A pesar del progreso técnico, la adopción masiva de la XR plantea desafíos para el bienestar físico y psicológico del usuario. La cinetosis, o mareo por simulación, sigue siendo una de las principales barreras para las sesiones prolongadas de RV.

Mecanismos y soluciones para la cinetosis

La cinetosis se produce por un conflicto sensorial: los ojos perciben movimiento en el entorno virtual, pero el sistema vestibular (oído interno) informa que el cuerpo está estático. Los síntomas incluyen náuseas, desorientación y fatiga ocular. Para mitigar esto, la industria ha implementado diversas soluciones:

- **Latencia Ultra-Baja**: Dispositivos de gama alta como el Apple Vision Pro (2026) han reducido la latencia de fotón a fotón a solo 12 milisegundos, eliminando el retraso entre el movimiento de la cabeza y la actualización

de la imagen.

- **Frecuencias de Refresco Elevadas**: El estándar de la industria se ha consolidado en 120 Hz, lo que proporciona una fluidez visual que engaña al cerebro de manera más efectiva.
- **Sistemas de Pantallas Varifocales**: Estos visores imitan la capacidad de enfoque natural del ojo humano, eliminando el conflicto de vergencia-acomodación que provoca fatiga visual extrema.
- **Uso de Rest Frames (marcos de descanso)**: La inclusión de elementos visuales estáticos en la periferia del campo de visión, como la cabina de un coche o el interior de un casco, ayuda al usuario a mantener el equilibrio.

Ergonomía del hardware y fatiga muscular

La evolución del diseño de los visores se ha centrado en el confort para su uso profesional a lo largo de toda la jornada laboral. Dispositivos como el Pico 4 Ultra Enterprise han distribuido el peso de forma equilibrada, montando la batería en la parte posterior de la cabeza, lo que reduce la presión sobre la cara y el cuello. El uso de lentes pancake ha permitido fabricar cascos más delgados y ligeros, lo que reduce la fatiga muscular acumulada durante sesiones de trabajo prolongadas en el metaverso industrial.

Marco legal, ética y privacidad en la computación espacial

La capacidad de los dispositivos de XR para recopilar datos biométricos detallados ha generado una intensa actividad regulatoria. Los visores

modernos capturan no solo el entorno del usuario, sino también sus patrones de mirada, expresiones faciales e incluso signos de estrés, lo que plantea riesgos significativos para la privacidad y la autonomía individuales.

El impacto de la Ley de IA de la UE y el GDPR

La Ley de IA (AI Act) ha establecido prohibiciones claras sobre el uso de sistemas de IA para el reconocimiento de emociones en contextos laborales y educativos. Esto limita significativamente el uso de las capacidades de seguimiento facial de los visores de XR para monitorear la productividad o el estado de ánimo de los empleados, permitiéndose únicamente para fines médicos o de seguridad críticos (véase la Tabla 8).

Tabla 8: Desafíos legales de la Ley de IA de la UE

Desafío Legal	**Implicación**	**Norma Relacionada**
Captura de datos de terceros	Los usuarios de gafas inteligentes son responsables de avisar a los transeúntes de que se está grabando.	GDPR (arts. 13 y 14) y Sentencia del ECJ C-422/24.
Reconocimiento emocional	Prohibido su uso para evaluar el desempeño laboral o escolar.	AI Act (Art. 5).

Responsabilidad por fallos	El software de XR se considera un producto, lo que hace al fabricante responsable de los daños.	Directiva sobre la responsabilidad por productos de la UE.
Datos biométricos	El seguimiento ocular se considera un dato sensible por la información que proporciona sobre la salud.	GDPR (Art. 9).

La captura involuntaria de datos de personas ajenas a la tecnología es un problema crítico. Las gafas inteligentes pueden grabar audio y vídeo de forma continua, vulnerando la privacidad de terceros que no han dado su consentimiento. En entornos corporativos, la introducción de estos sistemas requiere la codeterminación obligatoria de los consejos de trabajadores, incluso si no se realizan grabaciones permanentes, debido a la presión psicológica que genera la posibilidad de ser monitoreado de forma constante.

Accesibilidad y diseño inclusivo en entornos inmersivos

La accesibilidad digital ha dejado de ser un complemento para convertirse en un requisito fundamental desde la fase inicial de diseño de cualquier experiencia de XR. La evolución de los estándares de la W3C, en particular la transición hacia WCAG 3, ha proporcionado un marco más flexible

y adecuado para entornos tridimensionales.

Estándares y características de accesibilidad

- **Multimodalidad**: Las interfaces deben permitir múltiples formas de entrada y salida de datos. Si un usuario no puede usar gestos manuales, el sistema debe ofrecer navegación por mirada o por voz.
- **Adaptación al Espacio**: Los menús y elementos de la interfaz deben ser redimensionables y posicionables según la comodidad del usuario. El modo sentado se ha convertido en una opción estándar para evitar que los usuarios con movilidad reducida tengan que realizar movimientos físicos extenuantes.
- **Subtítulos Espaciales y Audio Descriptivo**: En entornos de 360 grados, los subtítulos deben permanecer visibles para el usuario, independientemente de su orientación, y el audio espacial se utiliza para guiar a las personas con discapacidad visual mediante pistas sonoras tridimensionales.
- **Haptics como Guía**: La retroalimentación háptica avanzada en trajes y guantes se utiliza para proporcionar señales táctiles sobre la proximidad de objetos virtuales o la correcta ejecución de una tarea, lo que beneficia a los usuarios con deficiencias auditivas o visuales.

El modelo de conformidad de WCAG 3. Introduce los niveles Bronce, Plata y Oro, midiendo el éxito en función de los procesos y de la experiencia real del usuario, en lugar de una lista de verificación técnica rígida. Esto permite que aplicaciones complejas de realidad mixta sean certificadas como accesibles con base en la capacidad del usuario para completar tareas críticas

de forma independiente.

La integración de la realidad virtual y la realidad aumentada en el tejido productivo y social marca el comienzo de la era de la computación ambiental. Hemos superado la fase en la que la tecnología era un accesorio y hemos entrado en una etapa en la que lo digital es una extensión natural de la cognición y de la capacidad física humana (Pérez et al., 2024). La capacitación técnica ha alcanzado niveles de eficiencia sin precedentes, reduciendo errores que en el pasado costaban fortunas y vidas humanas. El diseño de interfaces, ahora espacial y adaptativo, respeta la psicología humana y se ajusta en tiempo real a las necesidades individuales.

En regiones como el Perú, la apuesta por la minería y la educación técnica inmersiva demuestra que la tecnología es un motor del desarrollo sostenible y de la competitividad global. Sin embargo, la sostenibilidad de este ecosistema dependerá de un equilibrio ético; el respeto por la privacidad de los datos espaciales y la garantía de que estas herramientas sean inclusivas para todas las personas son los pilares que definirán la madurez de la sociedad digital hacia 2030.

Conclusión

Esta investigación sobre las tecnologías emergentes en ingeniería de sistemas ofrece reflexiones clave sobre el estado actual y las perspectivas futuras de la disciplina. A lo largo del documento, se analiza cómo la convergencia de distintas innovaciones no solo mejora los procesos existentes, sino que también está redefiniendo los fundamentos de la arquitectura tecnológica a nivel mundial.

Una de las conclusiones más destacadas de este estudio es que el valor real de las tecnologías emergentes no radica en su uso aislado, sino en su interoperabilidad. La integración de la Inteligencia Artificial (IA) con el Internet de las Cosas (IoT)—el concepto de AIoT—, respaldada por la seguridad y la trazabilidad que ofrece la Blockchain, está generando ecosistemas autónomos capaces de tomar decisiones en tiempo real con una precisión nunca antes vista. La ingeniería de sistemas moderna ya no se centra en componentes individuales, sino en la coordinación de sistemas complejos y

La investigación destaca un cambio crucial: la transición de la computación centralizada en la nube al Edge Computing. Esta descentralización es esencial para aplicaciones que requieren baja latencia, como la telemedicina y los vehículos autónomos. Al mismo tiempo, la computación cuántica surge como la próxima frontera importante, prometiendo resolver problemas de optimización y de criptografía que actualmente superan las capacidades de la arquitectura de von Neumann.

No podemos discutir los avances tecnológicos sin afrontar los desafíos asociados. Esta obra destaca que la ciberseguridad debe integrarse desde el

diseño (Security by Design), en lugar de ser una capa adicional posterior. Además, la ética en los algoritmos de IA y la sostenibilidad energética de los centros de datos se convierten en pilares de una práctica profesional responsable. El ingeniero de sistemas en el siglo XXI debe, ante todo, ser un defensor de la integridad y del impacto social de la tecnología.

Este libro finalmente resalta cómo ha evolucionado el rol del ingeniero de sistemas. La velocidad a la que las tecnologías "emergentes" se convierten en "estándar" requiere una mentalidad de aprendizaje permanente (Lifelong Learning). El profesional de hoy necesita una visión integral que combine habilidades técnicas avanzadas con un buen entendimiento del negocio y una sensibilidad humanista para liderar el cambio.

La tecnología ya no es neutral; sus efectos inciden en la estructura social. Esta investigación señala que la ética debe dejar de ser solo un complemento retórico y convertirse en un requisito técnico. Se ha identificado que reducir los sesgos en los modelos de aprendizaje automático y mejorar la transparencia de la caja negra de la IA son fundamentales para prevenir la discriminación automática. El ingeniero de sistemas tiene la responsabilidad de liderar un diseño centrado en el ser humano, asegurando que la privacidad de los datos sea un derecho inviolable y que la autonomía de los sistemas no ponga en riesgo la dignidad ni la seguridad de los usuarios.

En conclusión, las tecnologías innovadoras mencionadas en este volumen no son solo herramientas, sino también impulsores de una nueva etapa industrial. La ingeniería de sistemas desempeña un papel crucial al liderar esta transformación, asegurando que el avance técnico se traduzca en sistemas más eficientes, justos y resistentes para la sociedad. El futuro no es algo que simplemente ocurre; es algo que diseñamos, programamos y

implementamos.

Bibliografía

Abdelmagid, A. M., & Diaz, R. (2025). Zero Trust architecture as a risk countermeasure in small–medium enterprises and advanced technology systems. *Risk Analysis,* 45, 2390–2414. https://doi.org/10.1111/risa.70026

Alnaim, A. K., & Alwakeel, A. M. (2025). Zero Trust Strategies for Cyber-Physical Systems in 6G Networks. *Mathematics*, *13*(7), 1108. https://doi.org/10.3390/math13071108

Araujo, M. S. d., Machado, B. A. S., & Passos, F. U. (2024). Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Applied Sciences*, *14*(5), 2116. https://doi.org/10.3390/app14052116

Armada Pacheco, J. M., Oseda Gago, D., Ramos Piñas, D., & Franklin Moises, G. Y. (2026). Gemelos digitales y mantenimiento predictivo en industrias manufactureras de Huancayo. *Revista Venezolana De Gerencia*, *31*(114), e3111421. https://doi.org/10.52080/rvgluz.31.114.21

Bautista Godínes, T. (2019). El lado humano de la ingeniería de sistemas: principios para la vida. *Revista Digital Universitaria,* 20(2). http://doi.org/10.22201/codeic.16076079e.2019.v20n2.a8

Chaparro-Cárdenas, S. L., Ramirez-Bautista, J. A., Terven, J., Córdova-Esparza, D. M., Romero-Gonzalez, J. A., Ramírez-Pedraza, A., & Chavez-Urbiola, E. A. (2025). A Technological Review of Digital Twins and Artificial Intelligence for Personalized and Predictive Healthcare. *Healthcare (Basel,*

Switzerland), *13*(14), 1763. https://doi.org/10.3390/healthcare13141763

Cipresso, P., Giglioli, I. A. C., Raya, M. A., & Riva, G. (2018). The Past, Present, and Future of Virtual and Augmented Reality Research: A Network and Cluster Analysis of the Literature. *Frontiers in psychology*, *9*, 2086. https://doi.org/10.3389/fpsyg.2018.02086

Comisión Económica para América Latina y el Caribe (CEPAL). (2021). Tecnologías digitales para un nuevo futuro (LC/TS.2021/43). Santiago: Naciones Unidas. https://repositorio.cepal.org/server/api/core/bitstreams/879779be-c0a0-4e11-8e08-cf80b41a4fd9/content

Dix Rhenals, L., Tobar Rosero, Óscar A., & Ruiz Castañeda, W. L. (2025). Ecosistema de Innovación en Ingeniería: Transformación Digital y Gestión de Laboratorios Universitarios. *Encuentro Internacional De Educación En Ingeniería*. https://doi.org/10.26507/paper.4647

Hasan, S. K. K., & Crawford, C. W. (2025). A new era for digital twins: progress and industry adoption. *Digital Twin*, *2*(4). https://doi.org/10.1080/27525783.2025.2555877

Inga Ortega, E. (2019). *Aplicaciones e innovación de la ingeniería en ciencia y tecnología.* Quito: Editorial Abya-Yala. https://doi.org/10.7476/9789978104910

Ipuz Patiño, D. C., Vargas Giraldo, E. N., & Sánchez Munevar, J. (2025). Realidad Aumentada y Realidad Virtual: Nuevas Oportunidades para la

Industria Gráfica. *Cuadernos Del Centro De Estudios De Diseño Y Comunicación*, (255). https://doi.org/10.18682/cdc.vi255.12185

Janaćković, G., Vranjanac, Ž., & Vasović, D. (2025). Enhancing Urban Resilience: Integrating Actions for Resilience (A4R) and Multi-Criteria Decision Analysis (MCDA) for Sustainable Urban Development and Proactive Hazard Mitigation. *Sustainability*, *17*(14), 6408. https://doi.org/10.3390/su17146408

Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. *Entropy (Basel, Switzerland)*, *25*(12), 1595. https://doi.org/10.3390/e25121595

Krejčí, J., Babiuch, M., Suder, J., Krys, V., & Bobovský, Z. (2025). Internet of Robotic Things: Current Technologies, Challenges, Applications, and Future Research Topics. *Sensors (Basel, Switzerland)*, *25*(3), 765. https://doi.org/10.3390/s25030765

Llanos-Ruiz, D., Abella-García, V., & Ausín-Villaverde, V. (2025). Virtual Reality in Higher Education: A Systematic Review Aligned with the Sustainable Development Goals. *Societies*, *15*(9), 251. https://doi.org/10.3390/soc15090251

López, H. L. L., Rodríguez, L. G. Q., González, M. del C. O., & Ramírez, M. I. T. (2024). Desarrollo Sustentable en la Currícula de Ingeniería en Sistemas. *REVISTA DELOS*, *17*(60), e2283. https://doi.org/10.55905/rdelosv17.n60-086

Lorenzoni, N., Simões de Almeida, R., Wimmer, D., Simbrig, I., Moscon, V.,

Carnelli, F., Sulkowski, N., Malaka, E. P., Schober, P., Michel, K., Sá, V. J., & Raich, M. (2025). Development of a Pandemic Resilience Competence Model for Healthcare Professionals-Individual and Organisational Aspects. *International journal of environmental research and public health*, *22*(5), 712. https://doi.org/10.3390/ijerph22050712

Magyari, A., & Chen, Y. (2025). Optimizing SPHINCS+ for Low-Power Devices. *Electronics*, *14*(17), 3460. https://doi.org/10.3390/electronics14173460

Martinez-Duque, D., Sánchez-Medina, I.I., Cabrera-Medina, J.M., & Clavijo-Bustos, N. (2021). Inclusión de ingeniería sostenible en el contexto regional. *Formación universitaria*, *14*(5), 11-18. https://dx.doi.org/10.4067/S0718-50062021000500011

Martín-Mariscal, A., Torres-Leal, C., Aguilar-Planet, T., & Peralta, E. (2025). The Role of Virtual and Augmented Reality in Industrial Design: A Case Study of Usability Assessment. *Applied Sciences*, *15*(15), 8725. https://doi.org/10.3390/app15158725

Muller, G., van Veen, L., & van den Aker, J. (2023). Systems Engineering Education: From Learning Program to Business Value. *Systems*, *11*(10), 510. https://doi.org/10.3390/systems11100510

Nativi, S., Mazzetti, P., & Craglia, M. (2021). Digital Ecosystems for Developing Digital Twins of the Earth: The Destination Earth Case. *Remote Sensing*, *13*(11), 2119. https://doi.org/10.3390/rs13112119

Norikane, Y., & Nishimura, H. (2025). Security and Resilience of a Data Space Based Manufacturing Supply Chain. *Systems*, *13*(8), 676. https://doi.org/10.3390/systems13080676

Pérez-Muñoz, S., Castaño Calle, R., Morales Campo, P. T., & Rodríguez-Cayetano, A. (2024). A Systematic Review of the Use and Effect of Virtual Reality, Augmented Reality and Mixed Reality in Physical Education. *Information*, *15*(9), 582. https://doi.org/10.3390/info15090582

Román-Salinas, R. V., Díaz-Martínez, M. A., Ruíz-Hernández, S., Cervantes-Zubirías , G., & Morales-Rodríguez , M. A. (2024). El internet de las cosas y la industria 4.0- Aplicaciones en el campo de la ingeniería industrial. *Revista UIS Ingenierías*, *23*(2), 111–130. https://doi.org/10.18273/revuin.v23n2-2024007

Salem, A.H., Azzam, S.M., Emam, O.E. et al. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *J Big Data,* 11, 105. https://doi.org/10.1186/s40537-024-00957-y

Usländer, T., Baumann, M., Boschert, S., Rosen, R., Sauer, O., Stojanovic, L., & Wehrstedt, J. C. (2022). Symbiotic Evolution of Digital Twin Systems and Dataspaces. *Automation*, *3*(3), 378-399. https://doi.org/10.3390/automation3030020

Xu, D., Gondal, I., Yi, X., Susnjak, T., Watters, P., & McIntosh, T. R. (2025). The Erosion of Cybersecurity Zero-Trust Principles Through Generative AI: A Survey on the Challenges and Future Directions. *Journal of Cybersecurity and Privacy*, *5*(4), 87. https://doi.org/10.3390/jcp5040087

Yaqub, M. Z., & Alsabban, A. (2023). Industry-4.0-Enabled Digital Transformation: Prospects, Instruments, Challenges, and Implications for Business Strategies. *Sustainability*, *15*(11), 8553. https://doi.org/10.3390/su15118553

Zhihan, L.V. (2023). Digital Twins in Industry 5.0. *Research,* 6, 0071. https://doi.org/10.34133/research.0071

De esta edición de “*Tecnologías emergentes en ingeniería de sistemas”*, se terminó de editar en la ciudad de Colonia del Sacramento en la República Oriental del Uruguay el 01 de marzo de 2026

EST. 2021 EMC
EDITORIAL MAR CARIBE

TECNOLOGÍAS EMERGENTES EN INGENIERÍA DE SISTEMAS

Ledy Milca Villacrez Mozombite
Norberto Ulises Roman Concha
Javier Elmer Cabrera Díaz
Oscar Benito Pacheco
Frida Mereyda López Córdova
Mario Bernabe Chauca Saavedra
Juan Carlos Lázaro Guillermo

ISBN: 978-9915-698-79-3
9 789915 698793

www.editorialmarcaribe.es