ARQUITECTURAS IOT POTENCIADAS CON INTELIGENCIA ARTIFICIAL Y CLOUD COMPUTING PARA LA TRANSFORMACIÓN DIGITAL DE SISTEMAS DE SEGURIDAD

IOT Architectures Powered by Artificial Intelligence and Cloud Computing for the Digital Transformation of Security Systems

José Eduardo Salazar Bonilla [1] · *Lídice Victoria Haz López* [2] · *Omar Leandro Almeida Navas* [3]

[1,3]Instituto Superior Universitario Bolivariano de Tecnología (ITB); [2]Universidad Estatal Península de Santa Elena (UPSE)
[1]jesalazar7@itb.edu.ec, [2]victoria.haz@hotmail.com, [3]olalmeida@itb.edu.ec

RESUMEN

La convergencia de la Inteligencia Artificial (IA) y el Cloud Computing ha redefinido el paradigma de los sistemas de seguridad física y lógica, transitando de modelos reactivos a ecosistemas proactivos y autónomos. Esta ponencia analiza el diseño y la implementación de arquitecturas de Internet de las Cosas (IoT) de última generación, específicamente estructuradas para la transformación digital en entornos de seguridad crítica. Esta transformación es imperativa si consideramos el crecimiento exponencial de la hiperconectividad; se estima que para el año 2030 habrá cerca de 30.000 millones de objetos conectados a internet a nivel global. Ante esta masificación, las arquitecturas tradicionales basadas netamente en la nube son insostenibles, haciendo obligatorio el procesamiento en el borde. Se examina la integración de modelos de Machine Learning y Deep Learning en el borde (Edge Computing) para la detección de anomalías en tiempo real, junto con la escalabilidad y capacidad de orquestación que ofrecen las plataformas de Cloud Computing modernas. A través de un análisis técnico de las publicaciones académicas y casos de uso industrial post-2022, se identifican las ventajas competitivas de estas arquitecturas: reducción drástica de la latencia en la toma de decisiones, optimización de recursos mediante análisis predictivo y una robustez superior ante vulnerabilidades de red. El estudio profundiza en componentes clave como la interoperabilidad de protocolos, la seguridad Zero Trust aplicada a nodos sensores y la gestión de grandes volúmenes de datos (Big Data) para la generación de inteligencia accionable. Finalmente, se presenta un esquema conceptual que sirve de guía para organizaciones en proceso de modernización, concluyendo que la triada IoT-IA-Cloud no es solo una mejora incremental, sino el pilar fundamental para la resiliencia y eficiencia de los sistemas de seguridad en la era de la industria 4.0.

Palabras claves:

arquitecturas IoT, inteligencia artificial, cloud computing, transformación digital, sistemas de seguridad, edge computing, análisis predictivo

FECHA DE RECEPCIÓN:
29 de mayo de 2026

FECHA DE ACEPTACIÓN:
16 de julio de 2026

FECHA DE PUBLICACIÓN:
03 de agosto de 2026

Volumen 01 No. 1. Agosto 2026, pp. 39-50

ABSTRACT

The convergence of Artificial Intelligence (AI) and Cloud Computing has redefined the paradigm of physical and logical security systems, shifting from reactive models to proactive and autonomous ecosystems. This paper analyzes the design and implementation of next-generation Internet of Things (IoT) architectures, specifically structured for digital transformation in critical security environments. This transformation is imperative given the exponential growth of hyperconnectivity; it is estimated that by 2030 there will be approximately 30 billion internet-connected objects globally. Faced with this proliferation, traditional architectures based solely on the cloud are unsustainable, making edge processing essential. The integration of Machine Learning and Deep Learning models at the edge (Edge Computing) for real-time anomaly detection is examined, along with the scalability and orchestration capabilities offered by modern Cloud Computing platforms. Through a technical analysis of academic publications and post-2022 industrial use cases, the competitive advantages of these architectures are identified: a drastic reduction in decision-making latency, resource optimization through predictive analytics, and superior robustness against network vulnerabilities. The study delves into key components such as protocol interoperability, Zero Trust security applied to sensor nodes, and the management of large volumes of data (Big Data) for generating actionable intelligence. Finally, a conceptual framework is presented to guide organizations undergoing modernization, concluding that the IoT-AI-Cloud triad is not just an incremental improvement, but the fundamental pillar for the resilience and efficiency of security systems in the era of Industry 4.0.

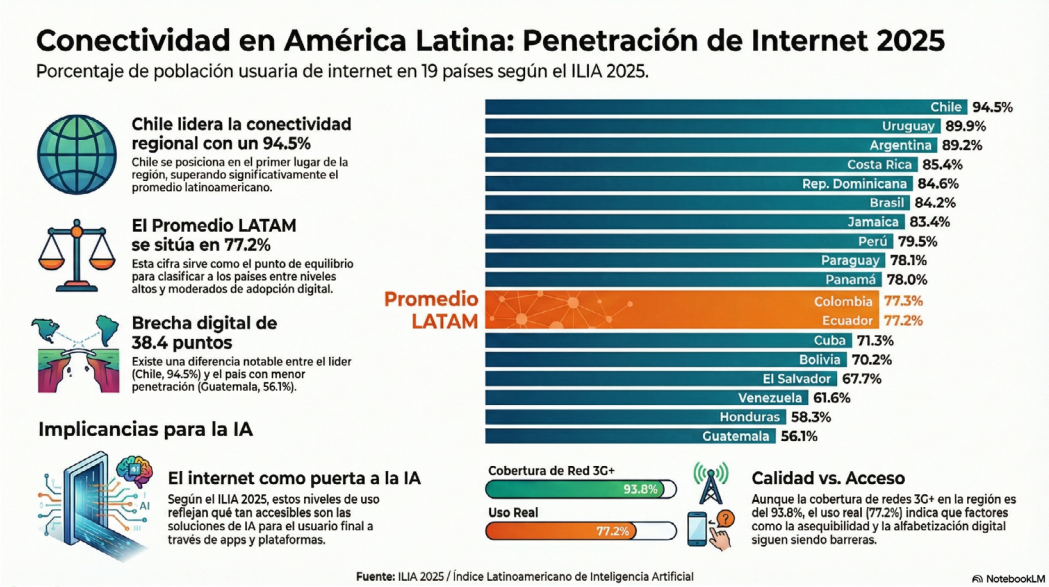
Keywords:

IoT architectures, artificial intelligence, cloud computing, digital transformation, security systems, edge computing, predictive analytics

INTRODUCCIÓN

El Internet de las Cosas (IoT) ha evolucionado de la simple conectividad a una infraestructura de inteligencia distribuida. En 2024, se estima que el gasto mundial en IoT alcanzó los 921 mil millones de dólares, impulsado por la necesidad de eficiencia operativa. (Statista, 2024) Las posibilidades actuales no se limitan al monitoreo; el campo de acción abarca desde la automatización industrial (IoT) hasta la gestión de infraestructuras críticas mediante Edge Computing, permitiendo que el procesamiento de datos ocurra en el origen, reduciendo la latencia y optimizando el ancho de banda en sistemas que no pueden permitirse retardos. La convergencia tecnológica permite que el IoT sea el pilar de la seguridad integral. En la seguridad física, facilita la vigilancia autónoma mediante sensores inteligentes; en la lógica, actúa como centinela en la detección de intrusiones en redes corporativas; y en la empresarial, garantiza la continuidad del negocio mediante el mantenimiento predictivo y la protección de activos. Según informes de seguridad de 2023, el 69% de las organizaciones en Latinoamérica sufrieron incidentes de seguridad, lo que subraya la urgencia de adoptar sistemas de monitoreo continuo y automatizado (ESET, 2023). A este escenario de vulnerabilidad se suma un crecimiento demográfico digital sin precedentes: América Latina alcanzará los 459 millones de usuarios de internet en 2025. Paralelamente, el costo anual de los ciberataques en Latinoamérica y el Caribe podría exceder los 90 millones de dólares para 2025, registrando un promedio de más de 18.5 millones de ataques por año. Este volumen de usuarios y amenazas demanda que la modernización de la infraestructura física vaya estrictamente acompañada de marcos regulatorios actualizados y robustos estándares de ciberseguridad integrados desde el diseño.

Figura 1
Porcentaje de penetración de Internet en América Latina y proyección de usuarios



Nota. Elaboración propia con base en datos del Índice Latinoamericano de Inteligencia Artificial y proyecciones regionales de conectividad digital en América Latina.

Como se observa en la Figura 1, la penetración de internet en América Latina presenta una tendencia sostenida de crecimiento, aunque con marcadas diferencias entre países, lo que evidencia una brecha digital estructural en la región (Soto, y otros, 2025). Esta asimetría en la conectividad no solo impacta el acceso a servicios digitales, sino que condiciona directamente la implementación de arquitecturas IoT, especialmente en entornos donde la latencia y la disponibilidad de red son factores críticos para la operación de sistemas de seguridad en tiempo real.

Latinoamérica enfrenta niveles críticos de inseguridad que actúan como un freno económico directo, costando a la región aproximadamente el 3.5% de su PIB anual (BID, 2023). La integración de Inteligencia Artificial en arquitecturas IoT permite pasar de una vigilancia pasiva a una prevención algorítmica. Mediante el análisis de patrones y detección de anomalías en tiempo real, la IA puede identificar comportamientos sospechosos o fallos de seguridad antes de que se conviertan en siniestros, optimizando los recursos limitados de seguridad pública y privada en la región. Este crecimiento acelerado de la conectividad en la región no solo incrementa las oportunidades de desarrollo digital, sino que amplía de forma proporcional la superficie de ataque en entornos tecnológicos. Diversos informes recientes evidencian que el número de incidentes de ciberseguridad en América Latina ha mantenido una tendencia creciente sostenida desde 2022, con incrementos anuales que superan el 20% en sectores industriales y de infraestructura crítica (ESET, 2023). Este fenómeno responde directamente a la expansión de dispositivos conectados, donde cada nodo IoT representa un potencial punto de vulnerabilidad si no se integra dentro de una arquitectura segura desde su diseño. En este contexto, la correlación entre hiperconectividad y exposición a amenazas no debe interpretarse únicamente como una consecuencia del crecimiento tecnológico, sino como un desafío estructural que exige la adopción de modelos de seguridad distribuidos, capaces de operar en tiempo real y bajo condiciones de alta demanda operativa. La región presenta trayectorias divergentes pero preocupantes. Ecuador cerró el 2023 con una tasa histórica de 47.25 homicidios por cada 100,000 habitantes, posicionándose entre los países más violentos de la región, a pesar de una ligera reducción proyectada del 14.7% para el cierre de 2024 (OECO, 2024). En contraste, países como México y Colombia mantienen tasas elevadas de criminalidad organizada, mientras que el cibercrimen ha crecido un 25% anual en la última década en toda la región, evidenciando que la inseguridad física y digital son ahora dos caras de la misma moneda (ESET, 2023). Los gobiernos latinoamericanos están comenzando a legislar para incentivar la transformación digital. En Ecuador, el Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial (presentado en junio de 2024) y la Política Nacional de Transformación Digital buscan crear un marco ético y técnico para el despliegue de estas tecnologías en el sector productivo (MINTEL, 2024). La adopción de políticas de Smart Policing y el fomento de ecosistemas digitales seguros son esenciales para que el IoT penetre en la población y las industrias de forma confiable. Para minimizar los impactos de la inseguridad, las empresas deben adoptar el modelo de Seguridad del IoT hacia 2026, enfocado en la resiliencia y el cifrado de extremo a extremo. Esto implica no solo instalar cámaras, sino integrar sistemas que utilicen Machine Learning para el control de acceso y la protección de perímetros, transformando la infraestructura de seguridad en una fuente de datos estratégicos que reducen pérdidas operativas y mejoran la confianza del inversor.

Volumen 01 No. 1. Agosto 2026, pp. 39-50

DESARROLLO

La evolución de los sistemas de seguridad electrónica hacia entornos digitalizados ha implicado su integración dentro del ecosistema de datos organizacional, dejando atrás el modelo tradicional de "circuito cerrado". En este contexto, el Internet de las Cosas (IoT) se posiciona como un habilitador clave para la convergencia entre seguridad física y ciberseguridad, permitiendo la generación, transmisión y análisis continuo de datos en tiempo real. Según el Worldwide ICT Spending Guide (IDC, 2024), el sector de seguridad física en América Latina se encuentra entre los principales impulsores de la adopción de tecnologías IoT, con proyecciones de inversión crecientes orientadas a la integración de capacidades de inteligencia artificial en el borde. Este fenómeno responde a la necesidad de reducir tiempos de respuesta ante incidentes, así como de mitigar riesgos asociados al movimiento lateral de amenazas dentro de infraestructuras conectadas (ESET, 2023). Para sustentar la viabilidad de las arquitecturas propuestas en este estudio, se realiza un análisis comparativo basado en métricas reportadas en la literatura reciente (2022–2025), considerando variables críticas como latencia de procesamiento, consumo de ancho de banda y eficiencia operativa en entornos de seguridad. Este enfoque permite evaluar las limitaciones de los modelos centralizados en la nube frente a arquitecturas distribuidas con capacidades de procesamiento en el borde. En este contexto, se propone una arquitectura IoT basada en un modelo Edge-to-Cloud, orientada a entornos de seguridad crítica, que integra procesamiento local mediante dispositivos inteligentes, protocolos de comunicación eficientes y mecanismos avanzados de seguridad como la microsegmentación y el modelo de Confianza Cero (Zero Trust).

A partir de este enfoque, la arquitectura propuesta se estructura en múltiples capas funcionales, cada una responsable de un conjunto específico de procesos dentro del ecosistema IoT. Esta segmentación permite no solo una mejor organización del flujo de datos, sino también la optimización de la latencia, la seguridad y la escalabilidad del sistema.

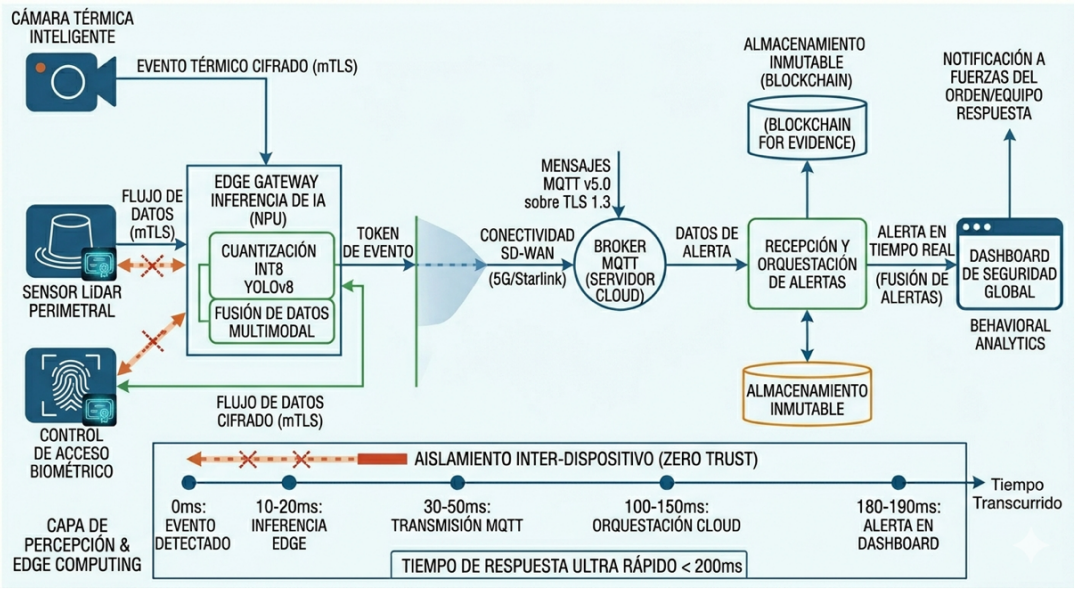
En términos generales, la arquitectura se divide en tres niveles principales: la capa de percepción y procesamiento en el borde, la capa de red y transporte, y la capa de aplicación y orquestación en la nube. Cada una de estas capas incorpora tecnologías y protocolos específicos que, en conjunto, permiten la operación eficiente de sistemas de seguridad en tiempo real.

- Capa de Percepción y Edge Computing (Hardware): La capa de percepción constituye el nivel inicial de la arquitectura IoT, encargada de la captura de datos desde el entorno físico mediante dispositivos sensores avanzados. A diferencia de los sistemas tradicionales de videovigilancia, esta arquitectura incorpora nodos inteligentes capaces de ejecutar procesos de inferencia local, lo que permite transformar datos en información útil desde el punto de origen. Estos nodos integran sistemas en chip (SoC) especializados, como plataformas de cómputo embebido optimizadas para cargas de trabajo de inteligencia artificial, permitiendo la ejecución de modelos de aprendizaje profundo —particularmente redes neuronales convolucionales (CNN)— directamente en el dispositivo. Esta capacidad reduce significativamente la dependencia de procesamiento en la nube y mejora los tiempos de respuesta ante eventos críticos. En términos funcionales, esta capa incluye dispositivos como sensores LiDAR para la detección de

Volumen 01 No. 1. Agosto 2026, pp. 39-50

presencia en perímetros, cámaras térmicas con analítica embebida para monitoreo en condiciones adversas, y sistemas de control de acceso biométrico que operan bajo protocolos seguros como OSDP (Open Supervised Device Protocol), en reemplazo de estándares heredados con limitaciones de seguridad. La incorporación de capacidades de inferencia en el borde permite que los dispositivos transmitan únicamente eventos relevantes en lugar de flujos continuos de datos, lo que contribuye a una reducción significativa del consumo de ancho de banda y mejora la eficiencia operativa del sistema. Este enfoque resulta especialmente crítico en entornos donde la latencia y la disponibilidad de red son factores determinantes para la operación de sistemas de seguridad en tiempo real.

Figura 2
Flujo de Datos y Latencia en el Procesamiento de Eventos Térmicos mediante AIoT



Nota. Esquema del flujo de datos desde la captura en el nodo sensor hasta la orquestación en la nube, incluyendo procesamiento en el borde e inferencia local.

- Capa de Red y Transporte (Conectividad): La capa de red y transporte es responsable de la transmisión eficiente y segura de los datos generados en la capa de percepción hacia los sistemas de procesamiento y almacenamiento. En arquitecturas IoT orientadas a entornos de seguridad crítica, esta capa debe garantizar baja latencia, alta disponibilidad y mecanismos robustos de protección frente a amenazas en tránsito. Para este propósito, la arquitectura propuesta emplea el protocolo MQTT (Message Queuing Telemetry Transport) en su versión 5.0, el cual opera bajo un modelo de publicación/suscripción que optimiza el intercambio de mensajes entre dispositivos distribuidos. A diferencia de protocolos tradicionales basados en solicitudes síncronas, MQTT reduce significativamente la sobrecarga de red, permitiendo una comunicación más eficiente en escenarios con recursos limitados o conectividad inestable. En términos de seguridad, la transmisión de datos se implementa sobre TLS 1.3, incorporando mecanismos de autenticación mutua (mTLS) que permiten validar tanto al cliente como al servidor mediante certificados digitales. Este enfoque fortalece la integridad y confidencialidad de la información, mitigando riesgos asociados a ataques de intermediario (Man-in-the-Middle) y a la suplantación de dispositivos dentro de la red.

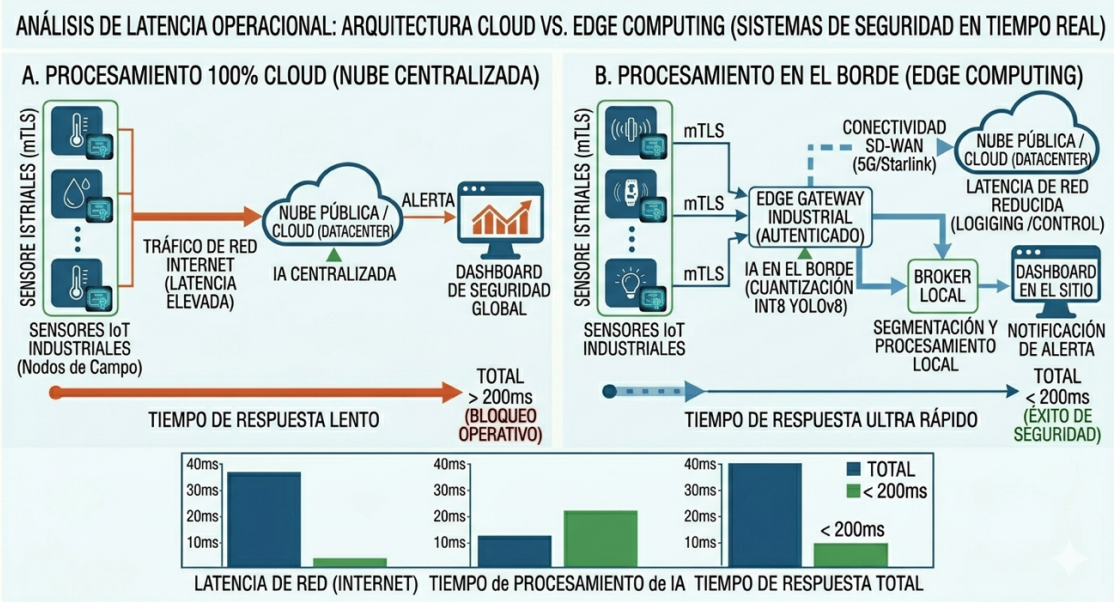
  Desde una perspectiva de infraestructura, la arquitectura contempla la coexistencia de múltiples tecnologías de conectividad, adaptándose a las condiciones heterogéneas de despliegue en América Latina. En entornos donde la estabilidad de la red fija es limitada, se integran soluciones como SD-WAN con enlaces redundantes que combinan conectividad terrestre y redes móviles de nueva generación, permitiendo mantener la continuidad operativa del sistema incluso en condiciones de degradación de la red. Esta capa no solo actúa como un canal de transmisión, sino como un componente estratégico para garantizar la resiliencia del sistema, asegurando que los eventos críticos generados en el borde puedan ser procesados y gestionados en tiempo real sin comprometer la disponibilidad ni la seguridad de la información.

- Capa de Aplicación y Orquestación (Software): La capa de aplicación y orquestación constituye el nivel superior de la arquitectura, encargada del procesamiento avanzado de datos, la gestión de eventos y la toma de decisiones en función de la información generada por las capas inferiores. En este nivel, los datos previamente filtrados y procesados en el borde son analizados mediante servicios escalables que permiten transformar eventos en inteligencia accionable. La arquitectura propuesta implementa un enfoque basado en microservicios y computación serverless, utilizando plataformas como AWS Lambda o Azure Functions, lo que permite procesar eventos de forma distribuida y elástica. Este modelo facilita la adaptación dinámica a variaciones en la carga de trabajo, optimizando el uso de recursos y reduciendo los tiempos de respuesta ante incidentes de seguridad. En este contexto, los modelos de inteligencia artificial desempeñan un rol central en la interpretación de los datos. A través de técnicas de análisis de comportamiento (Behavioral Analytics) y fusión de datos provenientes de múltiples sensores, el sistema es capaz de identificar patrones complejos y distinguir entre actividades normales y potenciales amenazas, mejorando la precisión en la detección de

Volumen 01 No. 1. Agosto 2026, pp. 39-50

eventos críticos. Adicionalmente, esta capa integra sistemas de gestión de video (VMS) y plataformas de monitoreo centralizado, permitiendo la visualización, correlación y auditoría de eventos en tiempo real. La interoperabilidad entre dispositivos y sistemas se ve reforzada mediante el uso de arquitecturas orientadas a servicios, facilitando la integración con infraestructuras existentes. Desde una perspectiva de seguridad y trazabilidad, se incorporan mecanismos avanzados para garantizar la integridad de los datos, incluyendo el uso de técnicas criptográficas para la generación de registros inmutables. Este enfoque resulta especialmente relevante en entornos donde la evidencia digital debe cumplir con estándares de validez legal y cadena de custodia. En conjunto, esta capa transforma la infraestructura de seguridad en un sistema inteligente capaz de anticipar riesgos, optimizar la toma de decisiones y mejorar la eficiencia operativa, consolidando el valor estratégico de la arquitectura IoT dentro de los procesos de transformación digital.

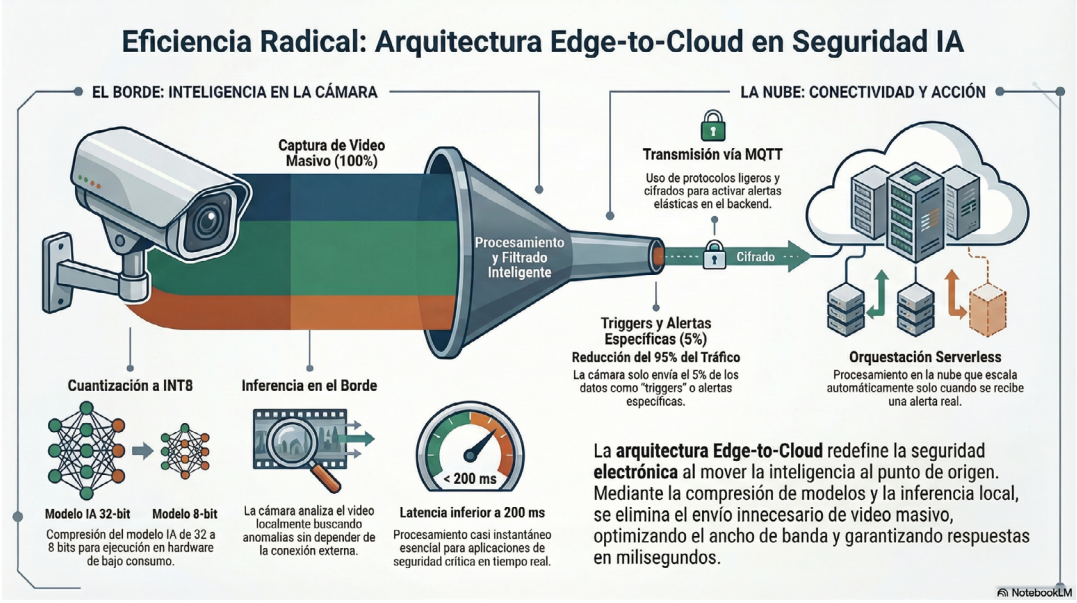
Figura 3
Análisis Comparativo de Latencia de Respuesta: Arquitectura Cloud vs. Edge Computing



Nota. El gráfico demuestra la superioridad del procesamiento en el borde (Edge) frente al modelo centralizado en la nube (Cloud), logrando tiempos de respuesta alcanzando tiempos de respuesta en rangos inferiores a 200 ms en escenarios optimizados.

Como se observa en la Figura 3, se presenta una comparativa de latencia entre arquitecturas centralizadas en la nube y modelos basados en Edge Computing, evidenciando las limitaciones de los modelos exclusivamente centralizados para aplicaciones de seguridad con requerimientos de baja latencia. Los Beneficios Estratégicos son la implementación puede contribuir a una reducción estimada de los costos operativos en un rango cercano al 20%–30% al automatizar la vigilancia. Además, permite el cumplimiento de normativas internacionales de cadena de suministro segura (World BASC Organization, 2022), vitales para las exportadoras ecuatorianas. La selección de protocolos y mecanismos de comunicación constituye un factor determinante en la resiliencia de los sistemas IoT, especialmente en entornos de seguridad de misión crítica. En escenarios con condiciones de red degradada frecuentes en zonas industriales, la arquitectura debe garantizar la continuidad operativa y la integridad de los datos frente a eventos adversos como ataques de denegación de servicio distribuido (DDoS), incluyendo casos ampliamente documentados como la botnet Mirai. En este contexto, la arquitectura propuesta adopta MQTT (Message Queuing Telemetry Transport) en su versión 5.0 como protocolo principal de comunicación, debido a su modelo de publicación/suscripción, el cual permite reducir significativamente la sobrecarga de red en comparación con enfoques tradicionales basados en HTTP. Adicionalmente, se implementa la funcionalidad Last Will and Testament (LWT), que permite detectar de manera inmediata la desconexión inesperada de dispositivos críticos, facilitando la identificación de posibles fallos o intentos de sabotaje en la red. Para el procesamiento de video, se emplea WebRTC como protocolo de transmisión en tiempo real, permitiendo alcanzar latencias inferiores a 500 ms en condiciones óptimas de red. Este enfoque resulta adecuado para aplicaciones de monitoreo remoto, donde la capacidad de reacción ante eventos es un factor crítico. Complementariamente, la seguridad en la comunicación se refuerza mediante el uso de TLS 1.3 con autenticación mutua (mTLS), garantizando la confidencialidad de los datos y evitando la incorporación de dispositivos no autorizados dentro del sistema. Desde la perspectiva de procesamiento de datos, la arquitectura prioriza la ejecución de modelos de inteligencia artificial en el borde, reduciendo la necesidad de transmitir grandes volúmenes de información hacia la nube. Para ello, se emplean técnicas de cuantización de modelos, permitiendo adaptar arquitecturas de detección como YOLOv8 a formatos optimizados (INT8), adecuados para su ejecución en dispositivos embebidos de bajo consumo. Este enfoque posibilita la implementación de inferencia local, donde los dispositivos únicamente transmiten eventos relevantes —como alertas o capturas específicas— en lugar de flujos continuos de video. Como resultado, se logra una reducción significativa del tráfico de red, que puede alcanzar valores superiores al 80% en comparación con arquitecturas centralizadas, dependiendo del tipo de aplicación y condiciones operativas.

Figura 4
Diagrama de la Arquitectura Inteligente Edge-to-Cloud y Zero Trust.



Nota. flujo de datos descentralizado donde el hardware de borde (cámara) ejecuta la cuantización del modelo de IA (reducción a INT8) procesando la inferencia localmente.

Como se observa en la Figura 4, esta lógica se integra dentro de una arquitectura Edge-to-Cloud, donde el procesamiento distribuido permite optimizar tanto la latencia como el consumo de recursos. La ejecución de modelos en el borde, combinada con un flujo de datos descentralizado, constituye un elemento clave para la eficiencia del sistema. A nivel de gestión y correlación de eventos, la arquitectura incorpora mecanismos de fusión de datos multimodal, permitiendo integrar información proveniente de distintos sensores —como sistemas de videovigilancia y dispositivos de control de acceso—. Este enfoque facilita la detección de escenarios complejos, como intrusiones no convencionales, mediante la correlación de eventos aparentemente independientes. En la capa de aplicación, el procesamiento de eventos se soporta mediante arquitecturas basadas en microservicios y contenedores, lo que permite escalar dinámicamente la capacidad del sistema ante incrementos en la demanda. Adicionalmente, se incorporan mecanismos de trazabilidad basados en técnicas criptográficas, que garantizan la integridad de los registros de eventos y su validez como evidencia digital en contextos legales. Finalmente, la arquitectura contempla la integración con infraestructuras físicas existentes mediante el uso de gateways industriales compatibles con protocolos legados, así como la incorporación de nodos actuadores inteligentes capaces de ejecutar acciones correctivas en tiempo real, como el control de accesos o la gestión de suministro eléctrico en zonas críticas.

CONCLUSIONES

La convergencia entre Internet de las Cosas (IoT), Inteligencia Artificial y Cloud Computing configura un cambio de paradigma en los sistemas de seguridad, permitiendo evolucionar desde modelos reactivos hacia arquitecturas distribuidas con capacidades de análisis en tiempo cercano al real. En este contexto, la incorporación de procesamiento en el borde (Edge Computing) se posiciona como un elemento clave para reducir la latencia, optimizar el uso de recursos y mejorar la capacidad de respuesta ante eventos críticos. El principal aporte de este trabajo radica en la propuesta de una arquitectura IoT basada en un modelo Edge-to-Cloud, diseñada para entornos de seguridad crítica, que integra inferencia local, protocolos de comunicación eficientes y mecanismos avanzados de protección como la microsegmentación y el modelo de Confianza Cero (Zero Trust). Este enfoque permite no solo mejorar la eficiencia operativa del sistema, sino también fortalecer su resiliencia frente a amenazas cibernéticas en entornos altamente distribuidos. En el contexto latinoamericano, y particularmente en escenarios industriales como los presentes en Ecuador, la adopción de estas arquitecturas representa una oportunidad para superar limitaciones estructurales relacionadas con la conectividad, la seguridad y la escalabilidad de los sistemas tecnológicos. La integración de estándares abiertos y tecnologías interoperables contribuye, además, a reducir la dependencia de proveedores y a garantizar la sostenibilidad de la infraestructura a largo plazo. Finalmente, la implementación de soluciones basadas en arquitecturas IoT distribuidas no solo tiene implicaciones técnicas, sino también económicas y estratégicas, al permitir la optimización de costos operativos y la mejora en la gestión de riesgos. En un escenario de crecimiento sostenido del ecosistema IoT a nivel global, estas tecnologías se consolidan como un componente fundamental para el desarrollo de sistemas de seguridad más eficientes, adaptables y alineados con los procesos de transformación digital de la región.

Volumen 01 No. 1. Agosto 2026, pp. 39-50

REFERENCIAS

BID. (2023). Banco Interamericano de Desarrollo. Obtenido de https://publications.iadb.org/publications/spanish/document/Los-costos-del-crimen--y-la-violencia-ampliacion-y-actualizacion-de-las-estimaciones-para-America-Latina-y-el-Caribe.pdf

CONECTA LATAM. (19 de Mayo de 2025). CONECTA LATAM. Obtenido de América Latina alcanzará 459 millones de usuarios de internet en 2025: https://www.conecta-latam.com/es/post/am%C3%A9rica-latina-alcanzar%C3%A1-459-millones-de-usuarios-de-internet-en-2025

ESET. (2023). ESET Digital Security Progress Report. Obtenido de https://web-assets.esetstatic.com/wls/es/articulos/reportes/cybersecurity-trends-2024-es.pdf

IDC. (2024). International Data Corporation. Obtenido de https://www.idc.com/getdoc.jsp?containerId=prUS51965524

IETF. (2024). Internet Engineering Task Force. Obtenido de https://datatracker.ietf.org/doc/html/rfc9431

MINTEL. (2024). Ministerio de Telecomunicaciones y de la Sociedad de la Información. Obtenido de https://observatorioecuadordigital.mintel.gob.ec/wp-content/uploads/2024/12/Proyecto-Acuerdo-Ministerial-Inteligencia-Artificial-Mintel-1.pdf

NIST. (2023). National Institute of Standards and Technology. Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

NU. CEPAL. (2025). Superar las trampas del desarrollo de América Latina y el Caribe en la era digital: el potencial transformador de las tecnologías digitales y la inteligencia artificial. CEPAL.

OECO. (2024). Observatorio Ecuatoriano de Crimen Organizado. Obtenido de https://oeco.padf.org/wp-content/uploads/2025/06/Boletin-anual-de-homicidios-intencionales-en-Ecuador-ajustado_compressed.pdf

Silberschatz, A., Baer Galvin, P., & Gagne, G. (2023). Operating System Concepts. Wiley.

SOCIUM. (17 de Noviembre de 2025). SOCIUM.CR. Obtenido de Infraestructura de Internet en LATAM 2026: El Año del Punto de Inflexión: https://socium.cr/blog-infraestructura-internet-latam-2026-analisis/

Soto, Á., Durán, R., Moreno, A., . . . L. (2025). Índice Latinoamericano de Inteligencia Artificial. Publicación de las Naciones Unidas.

Statista. (2024). Internet of Things (IoT) connected devices worldwide. Obtenido de https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

World BASC Organization. (2022). Norma y Estándares Internacionales BASC V06. Obtenido de https://www.wbasco.org/es/documento/guia-de-implementacion-norma-y-estandares-basc-v6-2022