# Exploración sobre de Network Digital Twin y herramientas de IA como apoyo a los pequeños ISP en LATAM - Version Final

Andrés Navarro C – Universidad Icesi

# *Resumen Ejecutivo*

La gestión de redes de telecomunicaciones ha alcanzado una complejidad sin precedentes, impulsada por la vertiginosa proliferación de dispositivos del Internet de las Cosas (IoT) y la demanda de servicios innovadores en las redes de quinta (5G) y sexta generación (6G). Las arquitecturas de red tradicionales y los enfoques de gestión y orquestación (MANO) se han vuelto insuficientes para abordar estos desafíos. En este contexto, emergen Network Digital Twin (NDT) y Zero Touch Management (ZTM) como paradigmas transformadores. NDT, una representación virtual en tiempo real de la red física, permite análisis predictivos, simulaciones de "qué pasaría si" y optimización en un entorno libre de riesgos. ZTM, por su parte, busca la autonomía total de la red, habilitando capacidades de auto-configuración, auto-monitorización, auto-curación y auto-optimización sin intervención humana.

El reporte profundiza tanto en los conceptos fundamentales, arquitecturas, capacidades, beneficios, desafíos y la sinergia inherente entre NDT y ZTM, integrando perspectivas de la literatura académica y organismos reguladores clave como ETSI, IETF e ITU.

Por otra parte, y dada la popularidad que tienen algunas herramientas de IA, y en especial la automatización de flujos, que puede ser una herramienta importante para los pequeños y medianos ISP, se analiza el uso y potencialidades de la IA y las herramientas basadas en flujos de IA, en las mejoras operacionales de los ISP pequeños y medianos. Una característica en común de estos pequeños operadores es que enfrentan una desventaja estructural significativa en la economía del tráfico de Internet. El análisis de costos revela que mientras los grandes operadores pueden "cachear" en CDN's aproximadamente el 58% del tráfico de servicios populares (como Google, Facebook o Netflix), los pequeños ISPs deben pagar por el total de su canal de datos. Esta disparidad genera un sobrecosto operativo que se acerca al 60% del valor de acceso al producto que proveen, lo que exige una búsqueda implacable de eficiencia en cada otra área del negocio para preservar la rentabilidad. Las herramientas de flujos automatizados basados en IA, como n8n y similares, pueden ayudar en el proceso de atención a usuarios y ayudar a solucionar algunos problemas técnicos, mejorando la eficiencia operacional y reduciendo costos para los ISP.

Allí en este aspecto es donde la automatización de flujos con herramientas de IA para mejorar el servicio al cliente y la detección de fallas en la red, representa una gran oportunidad, que es abordada en el documento.

Finalmente, se muestran los resultados de una encuesta realizada entre ISP, acerca de su visión y uso de herramientas de automatización, gestión de redes e Inteligencia Artificial en la

operación del negocio, lo que da una muy reducida idea de su visión acerca del uso de herramientas como NMS, Gemelos Digitales o flujos automatizados con IA.

# 1 Introducción

Los prestadores de servicios de Internet de tamaño pequeño y mediano (más conocidos como ISP por la sigla en inglés), que para efectos de este documento se refiere a los de menos de 30.000 usuarios, aunque el límite es elástico y borroso, son quienes llevan la conectividad a poblaciones pequeñas y a los lugares donde los grandes operadores globales no logran llegar. En Colombia, se estima que el número de pequeños y medianos ISP puede oscilar entre 3000 y 7000, según las cifras que se revisen; ABRINT en Brasil estima que puede haber cerca de 17000 ISP's en el país, y los números pueden ser igual de variables en los diferentes países de América Latina. Aunque hay también una gran variedad de tecnologías que incluyen redes PON y redes punto-multi punto basadas en espectro no licenciado, hay factores comunes donde se puede aplicar conceptos de gestión avanzada de red, Gemelos digitales y los conceptos que se abordan en los apartados siguientes.

## 1.1 Contexto de la Evolución de las Redes (5G y 6G)

La infraestructura de red global se encuentra en una fase de evolución acelerada, impulsada por la demanda exponencial de conectividad y servicios avanzados. La rápida proliferación de dispositivos inteligentes del Internet de las Cosas (IoT) y la creciente necesidad de servicios orientados a negocios en las redes 5G y las futuras redes 6G han generado una complejidad de gestión sin precedentes. Esta complejidad se manifiesta en la necesidad de integrar capacidades multidimensionales, incluyendo computación, detección e inteligencia, para soportar servicios emergentes como la comunicación holográfica, la interacción inteligente y la detección y comunicación integradas en 6G. Se espera que estas nuevas tecnologías aumenten drásticamente el número de terminales y la cantidad de funciones y servicios de red para 2040[1].

Los enfoques convencionales de gestión y orquestación de redes (MANO) se han revelado incapaces de seguir el ritmo de estos requisitos en constante cambio. La gestión manual de redes complejas y heterogéneas se ha vuelto ineficiente y propensa a errores, lo que subraya la urgencia de una transformación fundamental en las metodologías operativas. Esta escalada de complejidad no es meramente cuantitativa, sino que implica una transformación cualitativa en la naturaleza de los servicios y la infraestructura. La integración de diversas capacidades y la dinámica inherente de las redes modernas exigen sistemas que puedan comprender y actuar de manera autónoma y en tiempo real. La gestión de red tradicional, que implica monitorizar, reparar y reconfigurar subsistemas de hardware y software, se ha vuelto insuficiente para la escala y la complejidad actuales de la red global, que conecta miles de millones de personas y dispositivos.[2], [3]

## 1.2 La Necesidad de Automatización y Representación Digital

Para abordar la creciente complejidad y satisfacer los estrictos requisitos de rendimiento de los sistemas 5G y futuros, la automatización total de la red y la gestión de servicios se ha vuelto indispensable. En este contexto, surge el concepto de Digital Twin (DT) y su aplicación específica en el ámbito de las redes, Network Digital Twin (NDT). NDT ofrece la capacidad de crear réplicas virtuales detalladas de sistemas físicos de red, permitiendo simular, monitorizar y optimizar su comportamiento en tiempo real, lo que se traduce en un salto significativo en la eficiencia operativa.[4]

Complementando a NDT, Zero Touch Management (ZSM)[5], [6] representa una visión ambiciosa para lograr un sistema de red totalmente autónomo. El objetivo de ZSM es que la red sea capaz de auto-configurarse, auto-monitorizarse, auto-curarse y auto-optimizarse, basándose en políticas y reglas de servicio, sin requerir intervención humana, o con una intervención mínima, utilizando herramientas de IA y monitoreo. Esto implica que todas las operaciones y tareas, desde la planificación y el despliegue hasta el aprovisionamiento, la monitorización o monitoreo y la optimización, se ejecuten de forma automática. La combinación de NDT y ZSM es una respuesta estratégica a la **"crisis de complejidad"** que enfrentan las redes modernas. NDT proporciona la capacidad de comprender y predecir el comportamiento de la red en un entorno seguro, mientras que ZSM proporciona los mecanismos para actuar de forma autónoma basándose en esta inteligencia. Sin NDT, ZSM carecería de la inteligencia predictiva y la validación de políticas necesarias para una autonomía fiable, y sin ZSM, NDT sería solo un simulador avanzado sin la capacidad de ejecutar acciones de forma autónoma.

## 1.3 Estructura del Documento

El presente informe se estructura para proporcionar una comprensión integral de NDT y ZTM. La Sección 2 detalla los conceptos fundamentales y las arquitecturas de NDT, explorando sus capacidades, beneficios y desafíos. La Sección 3 se centra en ZTM, sus principios, la importancia para las redes de próxima generación y sus mecanismos de automatización. La Sección 4 analiza la sinergia entre NDT y ZTM, destacando cómo se complementan y cómo la inteligencia artificial y el aprendizaje automático actúan como el nexo integrador., la Sección 5 aborda las perspectivas regulatorias y de estandarización, así como los desafíos y las direcciones futuras para la implementación de estas tecnologías transformadoras. La sección 6 aborda el uso de herramientas basadas en flujos de IA para la mejora operativa del negocio, y la sección 6 describe los resultados de encuestas y entrevistas con ISP.

# 2 Network Digital Twin (NDT): Conceptos Fundamentales y Arquitectura

## 2.1 Definiciones y Evolución del Concepto de Digital Twin en Redes

El concepto de Digital Twin (DT) tiene sus raíces en la industria manufacturera, con antecedentes que se remontan al programa Apolo de la NASA en los años 70, donde se utilizaban réplicas físicas de vehículos espaciales para monitorizar sus condiciones en misión. Sin embargo, la definición formal de DT fue propuesta por Michael Grieves en 2003, describiéndola como una "representación digital virtual equivalente a los productos físicos". Este concepto fue posteriormente adoptado y ampliado por la NASA en 2012 para la gestión de la salud de aeronaves, integrando simulaciones de ultra-alta fidelidad con datos operativos y el historial de mantenimiento para replicar la vida de su contraparte física.[7]

La aplicación del DT al ámbito de las redes dio origen al Network Digital Twin (NDT). NDT se define como una "representación digital utilizada en el contexto de la red y cuya contraparte física es una red de datos" según el Internet Research Task Force (IRTF)[8]. De manera similar, la Unión Internacional de Telecomunicaciones (ITU) lo describe como una "representación virtual de una red física"[9], [10]. El objetivo primordial de NDT es representar las interacciones complejas entre los componentes de red, tanto virtualizados como físicos. A diferencia de los objetos físicos estáticos o de ciclo de vida más predecible en la manufactura, las redes son sistemas intrínsecamente dinámicos, distribuidos y heterogéneos. La migración del concepto de DT a las redes no es trivial y requiere una adaptación fundamental para capturar no solo la topología y configuración, sino también los estados operativos en tiempo real, las interacciones complejas entre componentes virtuales y físicos, y la capacidad de predecir el comportamiento futuro bajo condiciones cambiantes. Esto transforma el NDT en un modelo vivo y predictivo, más allá de una simple réplica estática. El proceso de "twinning" es el que crea y mantiene el NDT, asegurando una alineación continua con el gemelo físico.

## 2.2 Componentes Clave de NDT

Para la implementación exitosa de NDT, las especificaciones de IRTF e ITU[8], [9]

identifican una serie de elementos clave que cooperan para constituir un modelo de emulación de red altamente interactivo con la red física o como una plataforma de simulación autónoma. Estos elementos son:

- **Datos:** Constituyen el requisito principal para NDT. Incluyen configuraciones de red, topologías, eventos históricos, estados operativos, control de acceso, mapeo de servicios en recursos e información ambiental. Estos datos, aunque a menudo estructurados, pueden presentarse en diversos formatos y ser heterogéneos. La recolección de datos puede ser directa desde los componentes de red o a través del plano de gestión de red. Un enfoque recomendado es la recolección de datos orientada a tareas o en función de cambios de estado, lo que reduce la sobrecarga de almacenamiento y procesamiento de datos históricos.[1]
- **Modelos:** Representan el estado y el comportamiento de un sistema, siendo fundamentales para la recolección, procesamiento, presentación y análisis continuo de datos. Se distinguen dos tipos principales:
  - **Modelos Básicos:** Caracterizan y relacionan datos de componentes de red, como topología, enlaces e información ambiental (por ejemplo, la temperatura en una sala de centro de datos).
  - **Modelos Funcionales:** Están más orientados a tareas específicas, como diagnóstico de red, predicción de estado, optimización de estrategias de gestión de recursos, orquestación de recursos e ingeniería de tráfico. Pueden ser generales o de propósito especial, y si no existe un modelo funcional adecuado para un nuevo escenario, se pueden agregar atributos de modelos existentes para desarrollar uno nuevo. Otros tipos de modelos incluyen modelos de servicio, modelos de datos, modelos de conjuntos de datos, matrices de transferencia y grafos de conocimiento[11].
- **Interfaces:** Se identifican según su función. Un tipo de interfaz recopila datos de componentes físicos y virtuales, ya sea directamente o a través del plano de operación o gestión de red. También controlan y configuran la red física basándose en el resultado de las validaciones de configuración de NDT, utilizando protocolos existentes como NETCONF, SNMP, OpenFlow y gNMI. Un segundo tipo de interfaz expone las capacidades de NDT a las aplicaciones y permite la comunicación entre múltiples DTs para el intercambio de datos, la sincronización de estados y la coordinación en la toma de decisiones, facilitando la creación de un NDT global o a nivel de sistema[12].
- **Mapeo:** Se utiliza para identificar y establecer la relación interactiva en tiempo real entre la red física y el gemelo, o entre dos gemelos. Este mapeo puede ser:
  - **Vertical (uno a uno):** Permite la sincronización continua entre la red real y su gemelo virtual mediante flujos continuos de datos.
  - **Horizontal (uno a muchos):** Permite la sincronización entre diferentes gemelos con intercambio de datos periódico u ocasional, por ejemplo, la

comunicación entre los DTs de segmentos en el Edge-Cloud Continuum (ECC). Es fundamental validar la fiabilidad de la representación virtual de la red y la precisión del mapeo de estados.[13]

- **Lógica de Aplicación:** Se refiere a las capacidades de NDT para la resolución de problemas, el diagnóstico de red, la simulación de configuraciones, la planificación de servicios potenciales, la mejora del rendimiento y la asignación óptima de recursos. Esta lógica es el punto donde la inteligencia, a menudo habilitada por IA/ML, se materializa para transformar los datos y modelos estáticos en acciones dinámicas y predictivas, cerrando el bucle de control. La efectividad de esta lógica depende directamente de la fidelidad de los datos y modelos subyacentes, así como de la capacidad del mapeo para mantener la coherencia entre el mundo virtual y el físico. Un error o una imprecisión en cualquiera de estos componentes base se propagaría y degradaría la calidad de las decisiones generadas por la lógica.

## 2.3 Arquitecturas de Referencia de Netowork Digital Twin

Diversos organismos de estandarización y grupos de investigación han propuesto arquitecturas de referencia para NDT, reflejando una evolución desde modelos conceptuales generales hasta diseños más especializados e integrados con capacidades avanzadas.

- **Arquitectura de Referencia General**[8]**:** Esta propuesta inicial de IRTF presenta una arquitectura NDT donde los componentes funcionales interactúan con una contraparte física que implementa lógica de software para acceder a datos y responder consultas de manera oportuna. Incluye modelos de mapeo de servicios y una capa de aplicación de red que interactúa con las instancias NDT para la simulación de operaciones de red típicas y la evaluación de posibles impactos de nuevas intenciones o políticas.
- **Arquitectura Mejorada :** Para abordar la distribución de usuarios y redes a gran escala, esta arquitectura mejora el modelo anterior. Permite a los usuarios sondear las funciones de la instancia NDT y acceder a los resultados de la simulación. Incorpora un Intérprete para comprender las demandas (intenciones) del usuario, un Modelo Gemelo que representa componentes y datos de interacción en un solo segmento o múltiples subredes, una Federación de Modelos que agrega el conocimiento de modelos de datos de más de un segmento, y una Verificación de Modelos que ajusta los modelos de aprendizaje. El Almacenamiento de Puntos de Datos guarda la información recuperada en una estructura alineada con el mapeo

del modelo de datos. El Controlador de Red se posiciona por separado de la instancia NDT, exponiendo interfaces para que los usuarios de NDT configuren la red física, monitoricen o implementen aplicaciones basadas en intenciones. Esta mejora subraya la necesidad de escalabilidad y flexibilidad para la adopción de NDT en entornos complejos como el Edge-Cloud Continuum (ECC).

- **Packet Network Digital Twin (PNDT)** [14] **:** Esta es una instancia dedicada de NDT para redes IP. Su característica principal es su capacidad para realizar predicciones, estimaciones, análisis y desarrollar políticas de optimización para diversos objetivos. A diferencia de otras arquitecturas, PNDT no recolecta datos históricos directamente de los componentes de red, sino que utiliza datos del plano de gestión de red. Un Digital Twin Interface (DTI) actúa como puente entre el plano de gestión de red y el PNDT. La especialización de esta arquitectura para redes IP demuestra la tendencia hacia gemelos digitales adaptados a dominios de red específicos.
- **Arquitectura de Red 6G basada en Digital Twin** [4]**:** Esta propuesta para las redes 6G combina la arquitectura de red con un Digital Twin Network (DTN). Divide la red 6G en dominios de Servicio, Lógico y Recurso, basándose en la arquitectura de tres capas de la Virtualización de Funciones de Red (NFV). Utiliza hipergrafos intra-dominio e inter-dominio para modelar las complejas reglas cambiantes de varios elementos en la arquitectura de red y sus relaciones con el suministro de servicios.
- **Arquitectura AI-Native Network Digital Twin** [15], [16]**:** Este marco propone una integración cooperativa de modelos de Inteligencia Artificial (IA) en los tres tipos de gemelos digitales: Usuario (UDT), Infraestructura (IDT) y Slice (SDT). El objetivo es facilitar la emulación del estado de la red, la abstracción de patrones de red y la toma de decisiones inteligentes en las redes 6G. Modelos como Redes Neuronales Recurrentes (RNN), Redes Neuronales Convolucionales (CNN), Redes Neuronales de Grafos (GNN), Aprendizaje por Refuerzo Profundo (DRL) y Modelos de Lenguaje Grandes (LLM) están embebidos de forma nativa para optimizar la gestión de la red.
- **Arquitectura de Digital Twin Network basada en Grafo de Conocimiento** [11]**:** Esta arquitectura de DTN se compone de una Capa de Red Física, un Data Lake, una Capa de Digital Twin y una Capa de Aplicación de Red. Propone un método de construcción de DTN basado en grafos de conocimiento, capaz de representar atributos de entidades y diversas topologías según la red física, y extraer relaciones complejas de la red.
- **Arquitectura para Redes Ópticas con Controladores SDN Cloud-Native**[12]**:** Esta arquitectura utiliza controladores SDN para desplegar NDTs, proporcionando una representación virtual de la red óptica física. Permite la validación de trayectos de luz ópticos dinámicamente desplegados y la gestión del ciclo de vida de NDT. Incluye un Digital Twin Entity Manager (DTEM) para gestionar el ciclo de vida de

NDT y controlar sus elementos a través de una plataforma de virtualización.

La evolución de estas arquitecturas NDT revela una clara progresión desde la replicación básica hacia la inteligencia embebida y la granularidad de dominio. El paso de modelos de red genéricos a modelos especializados, como PNDT, y la integración nativa de IA/ML, como en AI-Native NDT, reflejan la creciente demanda de precisión y autonomía. Esta progresión subraya la necesidad de una capacidad de auto-organización y auto-optimización desde el diseño mismo de la red.

## 2.4 Capacidades y Beneficios de NDT

Los Network Digital Twin (NDT) ofrecen un conjunto de capacidades transformadoras que aportan beneficios significativos a la gestión y operación de redes, impulsando la eficiencia, la innovación y la resiliencia.

- **Análisis de Rendimiento en Tiempo Real y Emulación:** NDT recopila datos de componentes físicos, virtuales y de software, lo que permite un análisis de rendimiento en tiempo real, emulación y control inteligente de la red física. Esta capacidad es fundamental para comprender el estado actual de la red con una granularidad y precisión sin precedentes.
- **Soporte a Operadores de Red (NOs/CSPs):** NDT apoya directamente los objetivos de negocio de los Operadores de Red (NOs) y Proveedores de Servicios de Comunicación (CSPs). Ayuda en la orquestación y optimización de recursos, y en la ejecución de servicios de acuerdo con los requisitos y la Calidad de Experiencia (QoE) esperada por el cliente.
- **Escenarios "What-If" y Validación sin Riesgo:** Una de las capacidades más transformadoras de NDT es la validación de configuraciones y políticas mediante la simulación en plataformas de prueba o en una porción reservada de la red de producción. Esto permite identificar configuraciones y políticas defectuosas antes de que afecten a la red real, sin poner en peligro los recursos operativos. Esta capacidad de probar cambios en un entorno virtual elimina el alto riesgo asociado con la introducción de nuevas tecnologías o servicios en redes de misión crítica, acelerando drásticamente el ciclo de vida de desarrollo y despliegue.
- **Soporte a Nuevos Enfoques de Gestión:** NDT habilita y mejora las técnicas de gestión de red avanzadas como la Red Basada en Intenciones (IBN) y la Gestión de Red y Servicios Zero-Touch (ZSM)[6]. Proporciona la validación anticipatoria y la información necesaria sobre el posible impacto de cada política o configuración en los estados de la red física.
- **Planificación y Toma de Decisiones Optimizada:** Al simular diversas configuraciones de funciones de red, el NDT fortalece las políticas de programación de recursos y los procedimientos de orquestación. Sugiere los estados óptimos de los componentes de red y el mapeo de los componentes de

aplicación para satisfacer los requisitos de usuario más estrictos en términos de QoS y QoE. El NDT puede combinar la adquisición de datos, el procesamiento de big data y el modelado basado en Inteligencia Artificial (IA) para evaluar el estado actual de la red, predecir tendencias futuras y organizar de manera más eficiente el mantenimiento predictivo.

- **Reducción de Costos y Riesgos Operativos:** Al permitir la prueba y validación en un entorno virtual, el NDT reduce significativamente los gastos asociados con la experimentación de nuevas tecnologías y mitiga los riesgos antes del despliegue real. También optimiza el costo total de operación de la red.
- **Visibilidad Completa del Sistema:** El NDT proporciona una vista exhaustiva de todo el sistema, abarcando el estado de los recursos físicos y virtuales, lo que facilita una gestión de red más informada y completa.
- **Optimización del Edge-Cloud Continuum (ECC):** NDT busca representar y optimizar el ECC, permitiendo la colocación de aplicaciones consciente del rendimiento y abordando las complejidades de este entorno distribuido.
- **Mantenimiento Predictivo y Diagnóstico Proactivo:** NDT permite la detección temprana de anomalías y fallos, lo que reduce el tiempo de inactividad y los costos de reparación, transformando el mantenimiento de una actividad reactiva en una proactiva.
- **Habilitador para 6G:** NDT es un habilitador clave para 6G, permitiendo la virtualización de redes 5G/6G, mejorando el tiempo de ejecución y validación, proporcionando resultados fiables, reduciendo costos, permitiendo la comunicación bidireccional y facilitando el análisis de segmentación de red.[4]
- **Optimización como Servicio (OaaS):** NDT se ha estudiado para OaaS en 5G/6G, facilitando la optimización y planificación para aplicaciones de terceros al permitirles ejecutar enfoques en el gemelo antes de la implementación.
- **Mejora de la Calidad de Experiencia (QoE) y Calidad de Servicio (QoS):** NDT se utiliza para analizar la QoE en redes 6G a través de Human Digital Twins (HDTs) y para mejorar la QoS en 6G mediante Digital Twin Function Virtualization (DTFV) basada en SDN.
- **Aprovisionamiento Adaptativo de Servicios:** NDT permite la agregación y orquestación de recursos para proporcionar servicios adaptativos y diferenciados, optimizando la asignación de ancho de banda y la programación del tráfico en tiempo real.
- **Generación de Datos Sintéticos:** NDT proporciona capacidades para la generación y captura de tráfico de red en un entorno controlado, lo que es crucial para el entrenamiento y prueba de componentes de ML con datos realistas. Esto facilita el etiquetado de grandes conjuntos de datos sin intervención humana y permite generar datos sintéticos de alta calidad para reemplazar datos reales, mejorando la seguridad y evitando la fuga de privacidad, especialmente en escenarios donde las comunicaciones están cada vez más cifradas y el contenido

real no puede ser accedido para el entrenamiento de ML.

- **Optimización del Consumo Energético:** NDT puede utilizar métodos de ML para optimizar el uso de energía de la red prediciendo cuándo y dónde el uso de energía es más alto. De esta manera, la red puede reconfigurarse para reducir el consumo de energía en esas áreas específicas. También puede optimizar los procesos de entrenamiento e inferencia de componentes de IA para reducir el consumo de energía de la red.

## 2.5 Desafíos Actuales y Limitaciones de NDT

A pesar de sus prometedoras capacidades, la implementación y adopción generalizada de Network Digital Twin (NDT) enfrenta varios desafíos significativos, especialmente en el contexto de las redes de próxima generación (NGN) y el Edge-Cloud Continuum (ECC).

- **Contextualización del Edge-Cloud Continuum (ECC):** Las especificaciones actuales de NDT tienen limitaciones en la contextualización del ECC. Principalmente, se enfocan en la perspectiva del Operador de Red (NO) y no abordan adecuadamente cómo beneficiar a otros *stakeholders* como Proveedores de Servicios (SPs), Proveedores de Plataforma (PPs) y clientes. Esto se debe a que NDT no representa completamente las implicaciones de los principios de las tecnologías nativas de la nube, como la conteinerización y la Arquitectura de Microservicios (MSA), lo que resulta en una falta de vistas específicas y granulares para estos actores. La complejidad del ECC, con su heterogeneidad, multidimensionalidad y capacidad variable de nodos computacionales geo-distribuidos, requiere una representación más detallada y adaptada a múltiples intereses.
- **Recopilación y Procesamiento de Datos:** La construcción de NDT requiere la recopilación de volúmenes masivos de datos multimodales (video, audio, logs de red), lo que impone una alta presión de tráfico en las redes móviles. Gestionar este flujo de datos sin causar congestión o pérdida de paquetes es un desafío considerable. Además, se necesita un procesamiento de datos escalable que equilibre la intensidad computacional con la precisión de los datos del gemelo digital y un bajo consumo de energía. Las simulaciones de alta fidelidad para predecir el comportamiento de la red aumentan aún más las demandas energéticas.
- **Seguridad y Privacidad:** La sincronización de grandes volúmenes de datos de la red real en el NDT inevitablemente aumenta la superficie de ataque, elevando el riesgo de fuga de información. Las preocupaciones sobre la privacidad del usuario son significativas, dada la recopilación continua de datos de comportamiento y rendimiento. La integración de IA/ML en NDT también introduce nuevas

vulnerabilidades, como ataques de inversión de modelo o envenenamiento de datos.

- **Selección y Adaptación de Modelos de Aprendizaje:** Los modelos de IA/ML utilizados en NDT pueden volverse obsoletos debido a la "deriva de datos", es decir, cambios inherentes en las características de los datos de la red provocados por la evolución del comportamiento del usuario, la interoperabilidad de los dispositivos y las demandas de servicio. Esto requiere una recalibración y actualización oportuna de los modelos para mantener la fidelidad del NDT.
- **Despliegue de NDT:** La implementación efectiva del marco de software NDT con todas sus funcionalidades prometidas es un desafío. Esto incluye cómo gestionar la sobrecarga de comunicación interna entre los componentes de NDT (repositorios de datos, modelos) y la comunicación externa con aplicaciones de terceros y la red física en segmentos distribuidos del ECC.
- **Fidelidad del Modelado y Estandarización:** La variabilidad, incertidumbre y ambigüedad inherentes al espacio físico dificultan la construcción de modelos virtuales de alta fidelidad que reflejen con precisión el comportamiento de la red. La mayoría de los modelos NDT existentes se centran en aspectos geométricos, con una carencia en el modelado de comportamiento y reglas. Además, la ausencia de un enfoque estandarizado para el modelado de sistemas DT obstaculiza la comprensión del dominio y del usuario, así como el flujo de información entre las etapas de desarrollo.
- **Confianza y Credibilidad:** Es fundamental establecer la confianza y credibilidad en los resultados producidos por los gemelos digitales, especialmente para aplicaciones de misión crítica donde las decisiones automatizadas tienen consecuencias de alto impacto. Esto requiere una Verificación, Validación y Cuantificación de Incertidumbre (VVUQ por su sigla en inglés) rigurosa, para la cual aún no existe un proceso estándar de reporte. La tensión entre la necesidad de una representación de alta fidelidad y la complejidad inherente de las redes dinámicas y distribuidas es una brecha crítica. Esta tensión se manifiesta en la dificultad para mantener la precisión de los modelos de IA/ML frente a la deriva de datos y en la falta de métodos estandarizados para validar la confianza de los gemelos digitales, lo que podría frenar su adopción en entornos de misión crítica.
- **Desafíos en Redes Ópticas Desplegadas en Campo:** Factores como entornos imperfectos (temperaturas/presiones fluctuantes), funciones de control específicas de diferentes proveedores, actividades humanas inesperadas, envejecimiento de dispositivos, amplia cobertura geográfica y variabilidad de fabricación contribuyen a la imprecisión de NDT en redes ópticas.
- **Escalabilidad a Redes Reales:** Los modelos de NDT deben funcionar bien en redes significativamente más grandes que las utilizadas para el entrenamiento, lo que a menudo implica lidiar con cantidades fuera de distribución (como mayores volúmenes de tráfico y capacidad de enlace), lo que podría deteriorar el

rendimiento del NDT. Esto es un problema que debe abordarse para crear soluciones listas para la producción.

- **Movilidad de Usuarios Móviles:** La movilidad de los usuarios móviles puede llevar a escenarios donde la sincronización directa entre los usuarios físicos y sus DTs no es factible, lo que requiere soluciones de migración de DT para mantener la funcionalidad y la actualización.

## 2.6 Zero Touch Management (ZTM): Hacia Redes Autónomas

### 2.6.1 Definiciones y Principios de ZSM

Zero Touch Management (ZTM), también conocido como Zero-touch Network and Service Management (ZSM)[2], [17], es un concepto fundamental que apunta a la automatización completa de la gestión de redes y servicios. Su objetivo principal es la creación de un sistema de red autónomo, capaz de operar sin intervención humana. Esto implica que la red debe ser capaz de auto-configurarse, auto-monitorizarse, auto-curarse y auto-optimizarse, basándose en políticas y reglas de servicio predefinidas. En la práctica, esto significa que todas las operaciones y tareas del ciclo de vida de la red, como la planificación, entrega, despliegue, aprovisionamiento, monitorización y optimización, se ejecutan de forma automática.

Los principios de diseño de la arquitectura ZSM, establecidos por ETSI[18], son cruciales para su funcionamiento autónomo y escalable:

- **Soporte para instalaciones autocontenidas y débilmente acopladas:** Este principio permite que los nuevos servicios y módulos puedan adaptarse, escalarse e implementarse de forma independiente, lo que mejora la agilidad y flexibilidad del sistema.
- **Portabilidad, reusabilidad y gestión de recursos y servicios neutrales al proveedor:** ZSM facilita la creación de soluciones que no están atadas a un proveedor específico, promoviendo un ecosistema más abierto e interoperable.[1]
- **Automatización de gestión de bucle cerrado**[19]**:** Este es el corazón de ZSM, permitiendo que la red alcance y mantenga un conjunto de objetivos sin intervención continua. El bucle cerrado implica una monitorización constante, un análisis de las desviaciones del objetivo y un ajuste continuo, lo que es fundamental para la auto-regulación de la red.
- **Separación de funciones de gestión del almacenamiento y procesamiento de**

**datos:** Esta separación asegura que los servicios puedan reanudarse de manera eficiente después de que se resuelvan los problemas, mejorando la resiliencia del sistema.

- **Abstracción de la complejidad de los recursos del dominio:** La complejidad interna de los recursos dentro de un dominio de gestión se oculta a los usuarios del servicio, simplificando la interacción y la gestión a nivel de servicio.
- **Coordinación de actividades de dominio de gestión y gestión de servicios E2E**[20]**:** La gestión de servicios de extremo a extremo (E2E) coordina las actividades de los dominios de gestión individuales y supervisa los servicios que abarcan múltiples dominios.
- **Exposición de interfaces basadas en intenciones**[18]**:** Estas interfaces proporcionan abstracciones de alto nivel, permitiendo que la red interprete el comportamiento deseado de las entidades y traduzca estas intenciones en acciones concretas.

El principio de "bucle cerrado" o “lazo cerrado” es el núcleo de ZSM, transformando la gestión de red de una serie de acciones discretas y a menudo manuales en un proceso continuo de auto-regulación. Esto es fundamental para la autonomía, pero también introduce desafíos complejos en la estabilidad y la validación de decisiones. Un bucle abierto implica que una acción se ejecuta y se asume que tendrá el efecto deseado, sin verificación continua. Un bucle cerrado, sin embargo, implica monitorización constante, análisis de la desviación del objetivo y ajuste continuo. Esto es lo que permite la "auto-X" (auto-curación, auto-optimización). Sin embargo, la complejidad de los bucles cerrados en un entorno de red dinámico es enorme: ¿cómo asegurar la estabilidad? ¿Cómo evitar oscilaciones o estados no deseados? ¿Cómo validar que las decisiones automatizadas son seguras y óptimas en todo momento? Estos son los desafíos inherentes al principio de bucle cerrado.

### 2.6.2 La Importancia de ZSM en Redes 5G y Más Allá

La relevancia de Zero Touch Management (ZSM) en el panorama actual y futuro de las redes 5G y más allá es innegable[5], respondiendo a la creciente complejidad y a las demandas de un mercado en constante evolución.

- **Respuesta a la Complejidad de la Red:** La explosión de dispositivos IoT y la aparición de nuevos servicios han disparado la complejidad de las redes móviles, haciendo que las técnicas de gestión tradicionales sean insuficientes. ZSM ofrece una solución para manejar esta complejidad de manera eficiente.
- **Agilidad en el Despliegue de Servicios:** ZSM es fundamental para el despliegue ágil y la gestión eficiente de nuevos servicios. Tecnologías habilitadoras clave como la Virtualización de Funciones de Red (NFV), las Redes Definidas por Software (SDN), la Segmentación de Red (Network Slicing - NS) y la Computación

de Borde de Acceso Múltiple (Multi-Access Edge Computing - MEC) encuentran en ZSM el marco para una implementación y operación óptimas.

- **Gestión en Entornos Multidominio:** ZSM permite la orquestación y gestión de redes que operan a través de múltiples dominios, trascendiendo los límites legales y organizativos. Esto es vital en un ecosistema donde diferentes proveedores y tecnologías deben coexistir y colaborar.
- **Reducción de Costos Operativos y Mejora del Rendimiento:** La automatización inherente a ZSM conduce a una reducción significativa de los costos operativos y a una mejora sustancial en la visibilidad del rendimiento de la red. Al minimizar la intervención humana, se optimizan los recursos y se reduce la probabilidad de errores manuales.
- **Satisfacción de Requisitos de Calidad de Servicio (QoS):** ZSM proporciona una solución robusta para mejorar el rendimiento de la red y satisfacer los diversos y estrictos requisitos de Calidad de Servicio (QoS) y Calidad de Experiencia (QoE) que demandan las aplicaciones y usuarios de las redes 5G y 6G.

ZSM no es solo una necesidad operativa para la eficiencia, sino un imperativo estratégico para la innovación y la monetización de servicios en el ecosistema 5G/6G. Al reducir la intervención humana, ZSM libera recursos y permite a los operadores concentrarse en la creación de valor. La capacidad de desplegar y gestionar servicios de forma ágil y rápida (sin intervención manual) es lo que permite a los operadores responder a las oportunidades de mercado y crear nuevos modelos de negocio (multi-dominio, multi-servicio, multi-tenencia). Esto transforma la gestión de red de un centro de costos a un habilitador de ingresos y un motor de innovación.

## 2.6.3 Arquitectura de Referencia de ZSM

La arquitectura de referencia de Zero Touch Management (ZSM) está meticulosamente diseñada para lograr una automatización completa de la gestión de redes y servicios, especialmente en entornos multidominio donde las operaciones pueden abarcar diversas fronteras organizativas y tecnológicas.

### 2.6.3.1 Componentes Clave de ZSM[2]:

- **Servicios de Gestión (Management Services):** Son el bloque de construcción fundamental de la arquitectura ZSM. Proporcionan capacidades a los consumidores a través de puntos finales de servicio estandarizados. La flexibilidad de estos servicios permite que los existentes se fusionen para crear nuevos servicios, soportando una alta abstracción y un mayor alcance en las capas superiores de la jerarquía de composición.
- **Funciones de Gestión (Management Functions):** Actúan como productores y consumidores de servicios de gestión. Una función es un productor si genera

capacidades y un consumidor si utiliza servicios de gestión.

- **Dominios de Gestión (Management Domains - MDs):** Clasifican las responsabilidades administrativas para establecer una "separación de preocupaciones". Cada MD federa servicios de gestión con las capacidades necesarias para controlar los recursos o servicios orientados a recursos dentro de su alcance. Algunos servicios pueden requerir aprobación, mientras que otros están siempre disponibles.
- **Dominio de Gestión de Servicios E2E (E2E Service Management Domain):** Es un MD único y crucial que se encarga de la gestión de servicios orientados al cliente de extremo a extremo (E2E). Combina servicios orientados a recursos de varios MDs, pero no controla directamente los recursos de infraestructura subyacentes.
- **Tejido de Integración (Integration Fabric):** Facilita la comunicación e interoperación entre las funciones de gestión. Esto incluye el descubrimiento, registro e invocación de servicios de gestión, así como la integración de servicios y capacidades de comunicación.
- **Servicios de Datos (Data Services):** Permiten a los consumidores registrados acceder y persistir datos de gestión compartidos a través de los servicios de gestión. Su diseño separa el procesamiento de datos de la persistencia, lo que mejora la eficiencia y la resiliencia.

#### 2.6.3.2 Interfaces ZSM:

- **Recopilación de Datos de Dominio/E2E (Domain/E2E Data Collection):** Estos sistemas monitorizan servicios y entidades gestionadas, proporcionando datos de fallos y salida en vivo para la automatización de bucle cerrado. Interactúan con los servicios de inteligencia, análisis y orquestación.
- **Análisis de Dominio/E2E (Domain/E2E Analytics):** Generan recomendaciones específicas del dominio y análisis de causa raíz/impacto de servicio E2E, incluyendo la generación de predicciones específicas del servicio.
- **Inteligencia de Dominio/E2E (Domain/E2E Intelligence):** Son responsables de impulsar la automatización inteligente de bucle cerrado, apoyando la toma de decisiones automatizada y permitiendo niveles variables de supervisión humana.
- **Orquestación de Dominio/E2E (Domain/E2E Orchestration):** Gestionan el ciclo de vida de los servicios y recursos, automatizando flujos de trabajo y procesos dentro de un dominio o a través de múltiples dominios.
- **Control de Dominio (Domain Control):** Controla individualmente cada entidad, permitiendo cambiar configuraciones o estados de un servicio consumido o una entidad controlada.

La distinción entre "Dominios de Gestión" y el "Dominio de Gestión de Servicios E2E"

es crucial para la escalabilidad y la "separación de preocupaciones". Esto permite el modularidad y el crecimiento independiente, un principio fundamental para gestionar la complejidad de las redes de próxima generación que abarcan múltiples proveedores y tecnologías. En redes tradicionales, la gestión suele ser monolítica o altamente acoplada. A medida que las redes se expanden a múltiples proveedores, dominios geográficos y tecnologías (ej. Edge, Core, Cloud), un enfoque centralizado se vuelve inviable. La separación de dominios permite que cada uno gestione sus recursos de forma autónoma, mientras que el dominio E2E orquesta los servicios que atraviesan estos dominios. Esto reduce la complejidad de cada parte, mejora la resiliencia (un fallo en un dominio no detiene la gestión global) y facilita la colaboración entre diferentes entidades (operadores, proveedores de servicios, etc.) sin exponer la complejidad interna de cada dominio.

### 2.6.4 Mecanismos de Automatización (A2A) en ZSM

La trayectoria de la gestión de redes de "automática" a "autónoma" (A2A) es un pilar central de Zero Touch Management (ZSM). La automatización se refiere a la ejecución de tareas sin intervención humana, abarcando desde procesos de negocio hasta la gestión de red, asignación de recursos y optimización de enrutamiento. El objetivo es alcanzar el nivel más alto de abstracción en la automatización, desarrollando sistemas autónomos capaces de percibir, razonar y actuar de forma independiente.

Para lograr esta autonomía, ZSM se apoya en varios mecanismos clave:

- **Automatización Dirigida por Políticas**[1]**:** Las políticas son conjuntos de reglas que guían el rendimiento de las tareas de forma automatizada. Actúan como puntos de activación que, una vez cumplidos, ejecutan las medidas de automatización para tareas específicas. Esto proporciona un marco estructurado para la toma de decisiones automatizada.
- **Basada en Intenciones (Intent-Based Networking - IBN)**[18]**:** En fases iniciales, la "intención" se usaba como sinónimo de gestión basada en políticas. Sin embargo, su significado ha evolucionado para referirse a objetivos de alto nivel y cambios de comportamiento que rigen las características autónomas del sistema de gestión. Las intenciones permiten a los operadores expresar el "qué" (el resultado deseado) en lugar del "cómo" (los pasos de configuración específicos), dejando que el sistema autónomo determine la mejor manera de lograrlo.
- **Gobernanza de Red:** Este mecanismo implica que el control de las tareas es asumido por la propia red de forma autónoma. Se logra definiendo funcionalidades y conceptos que permiten a la red gestionar sus propios recursos e infraestructura, reduciendo la dependencia de la intervención humana.
- **Estabilidad de Red:** A medida que las funciones autónomas operan concurrentemente, pueden surgir conflictos o competencia por los recursos de red,

lo que podría llevar a inestabilidad. La estabilidad de red define condiciones y medidas preventivas para coordinar y gestionar estas funciones autónomas concurrentes, asegurando un funcionamiento eficiente y armonioso.

- **Aprendizaje por Refuerzo (Reinforcement Learning - RL):** A diferencia del aprendizaje supervisado o no supervisado que se basan en datos históricos, el RL implica que un agente de software interactúa con el sistema, aprende de las consecuencias de sus acciones (recompensas o penalizaciones) y crea una política óptima para lograr una tarea. Esto permite a la red aprender y adaptarse a entornos dinámicos y condiciones no previstas.
- **Aprendizaje por Transferencia (Transfer Learning):** Para abordar los desafíos de la disponibilidad de grandes volúmenes de datos y la complejidad computacional de entrenar algoritmos de ML desde cero, el aprendizaje por transferencia reutiliza el conocimiento (por ejemplo, pesos optimizados de redes pre-entrenadas) de una tarea o dominio a otro. Esto reduce la complejidad computacional y la necesidad de grandes cantidades de datos para el entrenamiento, acelerando el despliegue de soluciones de automatización.
- **Modelos de Lenguaje Grandes (LLMs):** Los LLMs pueden generar, verificar y configurar automáticamente dispositivos de red basándose en intenciones expresadas en lenguaje natural. Pueden crear interfaces conversacionales para la gestión de red, permitiendo a los operadores consultar el sistema usando lenguaje natural y recibir explicaciones comprensibles de decisiones impulsadas por IA. También pueden mejorar la automatización de la gestión del rendimiento y el análisis de la causa raíz, contribuyendo a los objetivos de ZSM como las capacidades de autogestión y la gestión basada en intenciones. Además, los LLMs pueden generar especificaciones formales, llamadas a API/funciones para SDN y protocolos de automatización, y desarrollar algoritmos de enrutamiento a partir de descripciones de alto nivel.

La transición de "automático" a "autónomo" en ZSM es una evolución de la ejecución de reglas predefinidas a la toma de decisiones adaptativa y auto-aprendizaje. RL y Transfer Learning [21] son fundamentales para esta evolución, permitiendo a la red aprender de la experiencia y adaptarse a condiciones no previstas, lo que es esencial para la verdadera autonomía y resiliencia. La automatización "automática" puede ser simplemente la ejecución de un script o una política fija. La autonomía "autónoma" implica que el sistema puede tomar decisiones en situaciones nuevas, aprender de sus errores y optimizar su comportamiento con el tiempo. Aquí es donde RL y Transfer Learning son cruciales. RL permite que un agente aprenda la mejor política a través de la interacción con el entorno (similar a cómo un humano aprende), mientras que Transfer Learning acelera este proceso al reutilizar conocimientos previos. Esto es un salto cualitativo, ya que permite a la red manejar la incertidumbre y la dinámica inherente de los entornos de 6G.

### 2.6.5 Gestión del Ciclo de Vida de Servicios E2E entre Dominios

La automatización de la gestión de red y el despliegue de servicios se ha convertido en un imperativo para los proveedores de servicios digitales, quienes buscan ofrecer servicios con mayor velocidad y eficiencia. Zero Touch Management (ZSM) aborda esta necesidad mediante la gestión del ciclo de vida de servicios de extremo a extremo (E2E) a través de múltiples dominios, un aspecto fundamental para la agilidad y la capacidad de respuesta de las redes de próxima generación[20].

El Dominio de Gestión de Servicios E2E es el responsable de coordinar y gestionar los servicios orientados al cliente y los servicios E2E a través de diversos dominios de gestión. Esta separación de responsabilidades reduce significativamente la complejidad general del servicio, permitiendo que la gestión E2E y la gestión de dominios operen de forma autónoma. La arquitectura ZSM, al separar la información operativa de las aplicaciones de gestión, proporciona un acceso fiable a los datos y ofrece servicios de datos entre dominios para la inteligencia de servicios y la gestión de red.

Los procesos clave del ciclo de vida de servicios E2E en ZSM incluyen:

- **On-boarding de Servicios:** Este proceso implica la adquisición de servicios E2E desde la fase de diseño del servicio. Consiste en añadir un nuevo modelo de servicio al catálogo de servicios del Dominio de Gestión de Servicios E2E. Puede incluir la creación de plantillas de servicio parametrizables para la instanciación concurrente de servicios. Los servicios de orquestación E2E y de dominio, junto con el Tejido de Integración ZSM y los Servicios de Datos ZSM, son fundamentales en esta fase.
- **Cumplimiento de Servicios (Service Fulfillment):** El Dominio de Gestión de Servicios E2E gestiona las instancias de servicio E2E desde su iniciación hasta su finalización. Esto abarca varias sub-fases:
    - **Instanciación de Servicios:** Solicita instancias de servicio de dominio para generar una instancia de servicio E2E, verificando su viabilidad, configurándola y probándola.
    - **Activación de Servicios:** Activa una instancia de servicio E2E, haciéndola operativa.
    - **Configuración de Servicios:** Modifica la configuración de una instancia de servicio E2E, solicitando al servicio de orquestación de dominio que ajuste las instancias de servicio de dominio afectadas.
    - **Desactivación de Servicios:** Desactiva una instancia de servicio E2E, impidiendo que siga prestando servicios.
    - **Desmantelamiento de Servicios:** Elimina una instancia de servicio E2E y libera todos sus recursos.
    - **Actualización de Inventario E2E:** Mantiene la información actualizada sobre

los recursos y las instancias de servicio de dominio gestionadas por el servicio E2E, rastreando eventos internos y recibiendo notificaciones de los dominios de gestión.

- **Aseguramiento de Servicios (Service Assurance):** Este proceso garantiza que el servicio E2E cumple con los requisitos de nivel de servicio (SLAs). Si el Dominio de Gestión de Servicios E2E no puede resolver un problema de calidad del servicio o si se requiere una acción, el problema se escala al consumidor del marco ZSM. Incluye la configuración del aseguramiento, la gestión de calidad del servicio y la gestión de problemas, así como el desmantelamiento del aseguramiento.

Dentro del Dominio de Gestión de Servicios E2E, diversos servicios operan para facilitar estas fases, incluyendo servicios de Inteligencia (para toma de decisiones y predicción), servicios de Recopilación (para datos de rendimiento E2E), servicios Analíticos (para detección de anomalías y análisis de condición) y servicios de Orquestación (para la ejecución de procesos operativos y la gestión de catálogos). Los servicios de datos entre dominios son cruciales, permitiendo el almacenamiento y el intercambio de información de gestión entre dominios, lo que apoya el análisis de big data y la inteligencia de servicios.

La gestión del ciclo de vida E2E es el puente que conecta la visión de alto nivel de ZSM con la realidad operativa de la red. La automatización de estos procesos críticos, desde el diseño hasta el aseguramiento, es lo que permite la agilidad y la capacidad de respuesta que las redes 5G/6G necesitan para monetizar nuevos servicios. La capacidad de una empresa de telecomunicaciones para lanzar y mantener nuevos servicios, como las *slices* de red, en cuestión de minutos o segundos, en lugar de días o semanas, representa una ventaja competitiva masiva y un requisito fundamental para la agilidad del mercado.

### 2.6.6 Aspectos de Seguridad en ZSM

La arquitectura de referencia del marco ZSM debe incluir características que permitan la protección de datos en uso, en tránsito y en reposo. Se espera un nivel óptimo de seguridad en las funciones de gestión, los servicios gestionados y los recursos de infraestructura. Debe garantizar la seguridad de los datos de gestión, la integridad de los datos, la gestión de los servicios y los recursos y funciones de infraestructura. Además, debe asegurar la disponibilidad de los recursos de infraestructura, los datos y las funciones de gestión. Los servicios gestionados deben incluir características de privacidad de datos personales como "privacidad desde el diseño" y "privacidad por defecto". Los usuarios de servicios autenticados deben aprobar el acceso a los servicios utilizando la arquitectura de referencia del marco ZSM, respaldando la capacidad de implementar automáticamente políticas de seguridad aceptables basadas en los servicios de gestión individuales y su estado de cumplimiento con respecto a los

requisitos de seguridad. También se debe apoyar la detección, el reconocimiento, la prevención y la mitigación automatizados de ataques/incidentes. Para evitar la propagación de vulnerabilidades y ataques, la arquitectura de referencia de la plataforma ZSM debe habilitar capacidades para supervisar/auditar las decisiones de ML/IA sobre cuestiones de privacidad y seguridad.

## 2.6.7 Amenazas de Seguridad en ZSM.

Como la mayoría de las tecnologías en la actualidad, el ZSM tiene diferentes amenazas de seguridad, que se describen en los apartados siguientes.

### 2.6.7.1 Ataques basados en ML/IA

- **Ataques de inversión de modelo:** Reconstruyen datos de entrenamiento a partir de parámetros del modelo para extraer datos privados y sensibles.
- **Ataques de extracción de modelo:** Utilizan parámetros del modelo extraídos mediante consultas al modelo.
- **Ataques de envenenamiento:** Explotan la fase de entrenamiento de los modelos de ML.
- **Ataques de evasión:** Explotan la fase de prueba de los modelos de ML.
- **Ataques de caja blanca:** El intruso tiene un conocimiento completo del modelo de clasificación.
- **Ataques de caja negra:** Los atacantes no conocen el modelo de clasificación, pero analizan su vulnerabilidad.

### 2.6.7.2 Amenazas de seguridad de API abiertas:

- **Ataques de parámetros:** Explotan datos transmitidos a través de una API (ej. inyecciones SQL, desbordamiento de búfer).
- **Ataques de identidad:** Intentos de acceso a una API objetivo utilizando credenciales comprometidas.
- **Ataques de denegación de servicio (DoS):** Sobrecargan los recursos esenciales de la API.
- **Ataques a aplicaciones y datos:** Incluyen fuga de datos, eliminación/modificación de datos, inyección de código.

### 2.6.7.3 Amenazas de seguridad basadas en intenciones:

- **Exposición de datos:** La automatización expone datos de interés de la aplicación que pueden ser interceptados.
- **Manipulación:** Cambios físicos realizados por un intruso en una interfaz o conexión.

#### 2.6.7.4 Amenazas de seguridad de red de bucle cerrado automatizadas:

- **Ataque Man-In-The-Middle (MITM):** Un intruso intercepta mensajes para escuchar o manipular el tráfico.
- **Ataques de engaño:** Un engañador convence a un objetivo para que acepte una versión incorrecta de la verdad.

#### 2.6.7.5 Amenazas debido a tecnologías de red programables (SDN y NFV):

- **Mayores riesgos con acceso programático a SDN:** Los riesgos aumentan al depender de aplicaciones de terceros.
- **Falta de aislamiento:** La información de control puede ser explotada para ataques.
- **Amenazas genéricas de virtualización y red:** NFV es susceptible a estas amenazas.
- **Vulnerabilidades en funciones de red virtualizadas (VNF):** Las VNFs pueden tener defectos que lleven a datos de monitorización inexactos.

#### 2.6.7.6 Posibles amenazas en la arquitectura del marco ZSM

- **Engaño de algoritmos de ML:** Los intrusos pueden generar entradas para engañar a los algoritmos de ML, llevando a decisiones incorrectas.
- **APIs inseguras:** Los atacantes pueden acceder o interferir con los servicios de ZSM.
- **Cuentas de consumidor comprometidas:** Un atacante puede manipular interfaces y servicios de orquestación.
- **Eventos de fallo fabricados:** Un atacante puede enviar un evento de fallo falso.
- **Secuestro de respuestas/redireccionamiento de tráfico:** Puede llevar a un ataque MITM (Man in the Middle).
- **Ataques a la base SDN/NFV:** La arquitectura ZSM es vulnerable a ataques como manipulación, suplantación de identidad, divulgación de información, denegación de servicio.
- **Datos de monitorización de VNF inexactos:** Las VNFs comprometidas pueden proporcionar datos inexactos.

#### 2.6.7.7 Mecanismos de Mitigación y Soluciones

Se han propuesto diversas soluciones para mitigar estas amenazas, incluyendo el uso de Deep Learning para mejorar la seguridad, modelos de ataque específicos como el Iterative Gradient Attack (IGA), y sistemas de detección de intrusiones basados en el tráfico. Además, se enfatiza la importancia de la autenticación de entidades, la evaluación de vulnerabilidades de algoritmos de ML, la prevención de la suplantación de aplicaciones SDN y la automatización impulsada

por políticas de seguridad. La integración de tecnologías como blockchain y mecanismos de confianza cero (Zero Trust) también se considera fundamental para fortalecer las defensas de ZSM.

## 2.7 La Sinergia entre Network Digital Twin y Zero Touch Management

La convergencia de Network Digital Twin (NDT) y Zero Touch Management (ZTM) es fundamental para la evolución hacia redes verdaderamente autónomas. NDT proporciona la inteligencia y el entorno de validación sin riesgos, mientras que ZTM se encarga de la ejecución autónoma, creando un sistema de automatización de bucle cerrado altamente eficiente y confiable.

### 2.7.1 NDT como Habilitador Clave para ZSM

Network Digital Twin (NDT) es un habilitador fundamental para la consecución de los objetivos de Zero Touch Management (ZSM). Actúa como el "cerebro" cognitivo y el "laboratorio de pruebas" de ZSM, proporcionando la inteligencia predictiva y la capacidad de validación sin riesgo que son absolutamente necesarias para que ZSM opere de forma verdaderamente autónoma y confiable, superando las limitaciones de la "caja negra" de la IA en la toma de decisiones.

- **Plataforma Avanzada de Emulación y Planificación:** NDT es una "plataforma avanzada para la emulación de red, sirviendo como herramienta para la planificación de escenarios, análisis de impacto y gestión de cambios". Esta capacidad permite a los ingenieros de red evaluar, modelar y refinar estrategias de optimización en un entorno virtual, libre de riesgos, garantizando que solo los cambios más efectivos se implementen en la red real.
- **Análisis de Causa Raíz y Sandbox de Pruebas:** NDT captura y agrega datos críticos para analizar las causas raíz de fallos de red, anomalías y vulnerabilidades. Además, ofrece un "sandbox" o entorno aislado para probar hipótesis, ejercitar escenarios de mitigación y validar conocimientos basados en datos sin afectar a los usuarios finales o la infraestructura de producción.
- **Inteligencia Predictiva para la Gestión:** NDT puede combinar la adquisición de datos, el procesamiento de big data y el modelado basado en Inteligencia Artificial (IA) para evaluar el estado actual de la red, predecir tendencias futuras y organizar de manera más eficiente el mantenimiento predictivo. Esta capacidad predictiva es vital para ZSM, ya que proporciona la validación anticipatoria y la información necesaria sobre los posibles impactos de cada política o configuración en los estados de la red física.

NDT actúa como el "cerebro" cognitivo y el "laboratorio de pruebas" de ZSM. Proporciona la inteligencia predictiva y la capacidad de validación sin riesgo que son absolutamente necesarias para que ZSM opere de forma verdaderamente autónoma y confiable, superando la limitación de la "caja negra" de la IA en la toma de decisiones. ZSM necesita ejecutar políticas de forma autónoma, pero esto requiere confianza y validación. NDT proporciona esto al simular escenarios de "qué pasaría si", probando políticas en un entorno virtual antes de su despliegue real. Esta capacidad de "sandbox" de NDT es crucial para que ZSM opere sin intervención humana y con alta fiabilidad. La integración de NDT en la gestión de red permite a los ingenieros evaluar, modelar y ajustar estrategias de optimización en un entorno libre de riesgos, asegurando que solo los cambios más efectivos se implementen en la red real, tras una validación y controles exhaustivos.

## 2.7.2 Integración de Inteligencia Artificial y Machine Learning en NDT y ZSM

La integración de la Inteligencia Artificial (IA) y el Aprendizaje Automático (ML) es un pilar fundamental tanto para Network Digital Twin (NDT) como para Zero Touch Management (ZSM), transformando la gestión de red hacia una autonomía inteligente. La evolución hacia arquitecturas "AI-Native" y la aplicación de AutoML marcan una madurez en esta integración, donde IA/ML no son solo herramientas complementarias, sino componentes arquitectónicos esenciales.

### 2.7.2.1 NDT y AI/ML

- **Mejora de la Gestión y Optimización:** Los modelos de IA/ML se integran en NDT para mejorar las capacidades de gestión de red, estimar el rendimiento, generar configuraciones óptimas y habilitar la computación distribuida en segmentos Edge, Multi-Access Edge Computing (MEC) y Cloud.
- **Modelos de Aprendizaje Comúnmente Utilizados:** NDT emplea una variedad de modelos de aprendizaje, incluyendo Redes Neuronales de Grafos (Graph Neural Networks o GNNs), Aprendizaje Federado (FL), Aprendizaje por Transferencia (TL), Aprendizaje por Refuerzo (RL) y Aprendizaje por Refuerzo Profundo (DRL), algoritmos Actor-Critic, Long Short-Term Memory (LSTM) y algoritmos de Proceso de Decisión de Markov (MDP). Otros modelos incluyen Support Vector Machine (SVM), Random Forest y K-Nearest Neighbors (K-NN) para tareas de clasificación y mantenimiento predictivo. Estos modelos aprenden sobre el entorno de red, los eventos y las interacciones de los componentes físicos y de software, informando políticas para la gestión de diversos escenarios y aplicaciones.
- **Comprensión y Procesamiento de Datos:** NDT aprovecha los modelos de

aprendizaje para comprender datos heterogéneos, procesar y clasificar datos de dominio de red, estimar diversas métricas de rendimiento y QoS, generar y probar políticas, y facilitar el entrenamiento continuo de los modelos.

- **Arquitectura AI-Native Network Digital Twin:** Este marco integra cooperativamente modelos de IA en los tres tipos de gemelos digitales (Usuario, Infraestructura y Slice) para la emulación del estado de la red, la abstracción de características de red y la toma de decisiones en las redes 6G.
- **GNNs para Modelado de Redes:** Las Redes Neuronales basadas en Grafos (GNNs) son particularmente adecuadas para el modelado de redes debido a su capacidad para procesar datos estructurados en forma de grafo. RouteNet-Fermi es una arquitectura GNN personalizada que predice con precisión el retardo, el jitter y la pérdida de paquetes, soportando modelos de tráfico arbitrarios y generalizando a escenarios no vistos[22]. Supera las limitaciones de las Redes Neuronales Multicapa (MLPs) y las Redes Neuronales Recurrentes (RNNs) en la generalización a cambios de topología o enrutamiento. Sin embargo, las GNNs presentan un factor limitante debido a su débil escalabilidad, lo que inevitablemente debe ser una compensación.
- **Grafos de Conocimiento (Knowledge Graphs):** Se utilizan para construir Digital Twin Networks (DTN), representando atributos de entidades y topologías complejas, y extrayendo relaciones de red. Esto permite una representación más rica y estructurada de la información de la red. El algoritmo de Extracción de Relaciones de Red (NRE), que combina LSTM y CNN, se propone para extraer relaciones complejas dentro de la red.
- **LLMs en DTs:** La integración de Modelos de Lenguaje Grandes (LLMs) en los marcos de Digital Twin mejora la seguridad del hardware mediante la comprensión del lenguaje natural y capacidades de razonamiento avanzadas. Esto permite interfaces conversacionales e interactivas, la generación de descripciones detalladas de escenas y la toma de decisiones basada en evidencia, lo que es crucial para la gestión de redes complejas.
- **IA Generativa (GAI):** La GAI se utiliza como un habilitador clave para generar datos de DT de alta fidelidad, aprendiendo la distribución compleja de los datos de red y utilizando información contextual (ambiental, de usuario, de servicio) para controlar el proceso de generación en diferentes escenarios. Esto permite una optimización impulsada por GAI, donde los simuladores generan datos de red de alta fidelidad para escenarios virtuales, y los optimizadores buscan soluciones óptimas.
- **Redes Neuronales Espiga (SNN):** Se investiga el rendimiento de los modelos GNN construidos utilizando técnicas SNN, que imitan el funcionamiento del cerebro humano y son adecuadas para capturar aspectos temporales de los datos.
- **Aprendizaje Automático Informado por la Física:** Se propone un enfoque híbrido que combina principios físicos con modelado basado en datos para el

modelado de dispositivos en redes desplegadas en campo, especialmente para componentes complejos como los amplificadores de fibra dopada con erbio (EDFA).

### 2.7.3 ZSM y AI/ML:

- **Toma de Decisiones Inteligente y Reducción de Intervención Humana:** El Aprendizaje Automático es fundamental para la toma de decisiones inteligente y la reducción de la intervención humana en ZSM.
- **Mecanismos de Automatización:** Los mecanismos de automatización de ZSM incluyen el Aprendizaje por Refuerzo y el Aprendizaje por Transferencia, que permiten a la red aprender de la experiencia y adaptarse a condiciones no previstas.
- **Automatización Impulsada por IA:** La IA impulsa la automatización de la red, aprovechando el big data y el ML para optimizar las operaciones.
- **AutoML:** La aplicación del Aprendizaje Automático Automatizado (AutoML) en Zero Touch Networks (ZTNs) se investiga para reducir los costos de gestión de red y mejorar el rendimiento, mostrando una precisión de predicción superior a la de ML tradicional.
- **LLMs para Gestión de Configuración:** Los LLMs pueden generar automáticamente configuraciones, verificarlas y configurar dispositivos de red basándose en intenciones expresadas en lenguaje natural, lo que es crucial para la gestión de configuración de red Zero Touch. También pueden usarse para generar especificaciones formales, llamadas a API/funciones para SDN y protocolos de automatización, y desarrollar algoritmos de enrutamiento a partir de descripciones de alto nivel.

La evolución hacia "AI-Native" en NDT y la aplicación de AutoML en ZSM marcan una madurez en la integración de IA/ML, pasando de ser herramientas complementarias a ser componentes arquitectónicos fundamentales. Esto subraya la necesidad de modelos de IA que no solo sean precisos, sino también eficientes, adaptables a la deriva de datos y explicables, para construir la confianza necesaria en la autonomía. A medida que la IA se vuelve más "nativa" y autónoma, la necesidad de confiar en sus decisiones se vuelve crítica. Esto impulsa la investigación en la "explicabilidad de la IA" (XAI) y la necesidad de mecanismos de validación robustos (VVUQ). Si la red va a operar de forma autónoma, los operadores necesitan entender por qué la IA tomó ciertas decisiones y confiar en que esas decisiones son correctas y seguras.

#### 2.7.3.1 Simulación y Emulación en el Contexto Conjunto

La simulación y la emulación desempeñan un papel crucial en la sinergia entre Network Digital Twin (NDT) y Zero Touch Management (ZSM), trascendiendo su función

tradicional como meras herramientas de análisis para convertirse en componentes operativos esenciales dentro de los bucles cerrados de automatización.

- **Habilitador de Escenarios "What-If":** La simulación es un "habilitador de escenarios 'What-If'" clave en NDT. Permite a los Operadores de Red (NOs) validar configuraciones y políticas, y evaluar su impacto en los recursos físicos sin poner en riesgo la red real. Este entorno de prueba virtual es fundamental para identificar configuraciones y políticas defectuosas antes de su despliegue, mitigando riesgos operativos.
- **Herramientas de Simulación Adecuadas:** Diversos simuladores son adecuados para la integración en NDT, ofreciendo flexibilidad para capturar el comportamiento de la red, emulación y prototipado de escenarios complejos. Entre ellos se incluyen Omnet++, Mininet, NS2/3, GNS3, 5G-LENA y Simu5G. Estos simuladores son capaces de replicar el comportamiento de los componentes de comunicación y los stacks de protocolos, siendo fácilmente integrables con marcos de trabajo de IA.
- **Complemento para Modelos de Aprendizaje:** La simulación puede generar datos de alta calidad utilizando modelos matemáticos, lo que complementa el entrenamiento de los modelos de aprendizaje automático y, en algunos casos, puede incluso eliminar la necesidad de un entrenamiento *a priori* con datos reales. Esto es particularmente valioso para generar datos de escenarios extremos o poco frecuentes que son difíciles de observar en redes de producción.
- **Marco de Emulación de Tráfico de Red:** Se ha propuesto un marco sistemático de emulación de tráfico de red para Digital Twin Network (DTN) con el objetivo de mantener la consistencia entre el tráfico de red físico y el del gemelo digital. Esto se logra mediante el uso de identificadores unificados y tecnología de red determinista, asegurando que el comportamiento del tráfico emulado sea fiel al real.
- **Pruebas de Ciberseguridad:** El gemelo digital puede utilizarse para estudiar el comportamiento de la red bajo diversas condiciones operativas, incluyendo ciberataques, en un entorno de bajo costo y riesgo cero. Esto permite evaluar y analizar cómo un sistema responde a los ciberataques en un entorno simulado.

La simulación y emulación en el contexto de NDT y ZSM no son solo herramientas de análisis, sino componentes operativos esenciales para el bucle cerrado de automatización. Permiten la "prueba de fallos" y la "optimización continua" en un entorno virtual, lo que es vital para la resiliencia y la evolución de las redes autónomas. Para que ZSM logre la auto-curación o auto-optimización, necesita una forma de validar las acciones correctivas o de mejora antes de aplicarlas en la red real. La simulación y emulación de NDT proporcionan este entorno seguro. Esto es especialmente crítico para la "resiliencia", ya que permite probar cómo la red se recuperaría de fallos complejos o ataques sin causar interrupciones reales. Además, al generar datos

sintéticos para entrenar modelos de IA/ML, la simulación ayuda a superar la escasez de datos de escenarios extremos en redes de producción, lo que es fundamental para la robustez de la IA en ZSM.

## 2.8 Perspectivas Regulatorias y de Estandarización

La estandarización es el puente crítico entre la investigación académica y la adopción industrial a gran escala de Network Digital Twin (NDT) y Zero Touch Management (ZSM). Sin estándares unificados, la interoperabilidad y la confianza en estas tecnologías se verían gravemente comprometidas, frenando su impacto transformador.

Diversos organismos de desarrollo de estándares (SDOs) están activamente involucrados en la definición de NDT y ZSM, sentando las bases para su implementación global, como se verá a continuación:

- **ETSI ZSM (European Telecommunications Standards Institute Zero Touch Network and Service Management):** Este grupo de especificación industrial (ISG) fue establecido en diciembre de 2017 con el objetivo de acelerar la estandarización de la arquitectura ZSM de extremo a extremo (E2E) y el despliegue de servicios basados en ZSM. ETSI ZSM ha publicado una serie de especificaciones (GS ZSM 001 a 010) que cubren desde los requisitos y escenarios (001), la arquitectura de referencia (002), la gestión y orquestación E2E de la segmentación de red (003), el panorama de actividades relacionadas (004), los mecanismos de automatización (005), hasta los aspectos de seguridad (010). Además, ETSI ZSM ha publicado el Grupo de Informe ETSI GR ZSM 015 [2] y la Especificación de Grupo ETSI GS ZSM 018, ambos centrados en Network Digital Twin para la gestión de red y servicios de toque cero (Zero Touch) mejorada.
- **IRTF NMRG (Internet Research Task Force Network Management Research Group):** El NMRG del IRTF ha sido fundamental en la definición conceptual de NDT. Define NDT como una "representación digital utilizada en el contexto de la red y cuya contraparte física es una red de datos". Sus borradores de Internet (como draft-irtf-nmrg-network-digital-twin-arch-11[8]) proporcionan una visión general de los conceptos, definiciones básicas, una arquitectura de referencia, escenarios de aplicación y discuten los beneficios y desafíos clave de esta tecnología.
- **ITU-T SG13 (International Telecommunication Union - Telecommunication Standardization Sector Study Group 13):** El Grupo de Estudio 13 de ITU-T se encarga del desarrollo de requisitos y arquitecturas para Redes Futuras y tecnologías de red emergentes. Ha aprobado y publicado la Recomendación ITU-T Y.3090, titulada "Digital twin network – Requirements and architecture"[9]. Además, el SG13 ha establecido Grupos de Enfoque como FG ML5G (Machine Learning para Redes Futuras, incluyendo 5G) y FG-Net2030 (Tecnologías para Red 2030),

que trabajan en posibles aplicaciones de IA/ML en redes[10].

- **3GPP (3rd Generation Partnership Project):** Aunque no tiene un grupo ZSM dedicado, 3GPP contribuye a la automatización de la red a través de sus grupos de trabajo de Aspectos de Servicio y Sistema (SA2 y SA5). Han propuesto el marco de Análisis de Datos de Red (NWDAF) para automatizar el intercambio de análisis de datos específicos de la segmentación de red, y han trabajado en la Arquitectura Basada en Servicios (SBA) para 5G, la gestión del rendimiento de Funciones de Red Virtualizadas (VNF) y la gestión de políticas de red automatizada. Hacia finales de 2023, 3GPP inició la investigación sobre NDT para delinear más claramente el objeto gemelo como la red de telecomunicaciones, empleando la terminología de NDT. 3GPP SA5 está trabajando en la definición de conceptos, términos, escenarios y requisitos de detección sin pérdidas en el sistema de gestión 3GPP.
- **TM Forum:** Desarrolla la visión de la Arquitectura Digital Abierta (ODA) [23] como un reemplazo ágil para las arquitecturas existentes de OSS/BSS (Operational Support System/Business Support System). ODA está estrechamente relacionada con la arquitectura ZSM, con guías de usuario que se correlacionan en la gestión de la segmentación de red para soportar múltiples y cambiantes modelos de negocio.
- **ONF (Open Networking Foundation):** ONF especifica la plataforma CORD (Central Office Re-architected as a Datacentre)[24] que aprovecha SDN, NFV y tecnologías de computación en la nube para construir redes ágiles de centros de datos de borde. También desarrolla modelos de datos y herramientas de software de código abierto que son útiles para desplegar redes basadas en SDN, incluyendo redes 5G y futuras, y especificaciones de interfaces de Redes Basadas en Intenciones (IBN) para SDN.
- **GSMA (Global System for Mobile Communications Association):** Ha iniciado el proyecto Network Slicing Taskforce (NEST)[25] para habilitar la interoperabilidad y armonizar el proceso de creación de *slices* a través de múltiples operadores. También define un conjunto completo de requisitos de servicio para la segmentación de red para diversas industrias verticales.
- **OASIS (Organization for the Advancement of Structured Information Standards):** El comité técnico TOSCA (Topology and Orchestration Specification for Cloud Applications) de OASIS[26] realiza tareas de estandarización relacionadas con la realización de ZSM. TOSCA define la descripción de servicios de red interoperables para nuevos servicios en la nube, permitiendo la portabilidad y la gestión automatizada entre múltiples proveedores de la nube.

La estandarización es el puente crítico entre la investigación académica y la adopción industrial a gran escala de NDT y ZSM. Sin estándares unificados, la interoperabilidad y la confianza en estas tecnologías se verían gravemente comprometidas, frenando su

impacto transformador. La fragmentación de enfoques y la falta de interoperabilidad son barreras históricas para la adopción de nuevas tecnologías en telecomunicaciones. Los esfuerzos de estandarización mencionados son cruciales para asegurar que NDT y ZSM puedan ser implementados de manera coherente y eficiente en un ecosistema de red cada vez más diverso y complejo.

## 2.9 Conclusiones de la sección

La gestión de redes de telecomunicaciones está experimentando una transformación fundamental, pasando de operaciones reactivas y centradas en el ser humano a sistemas proactivos, autónomos y basados en datos. Esta evolución es una respuesta directa a la creciente complejidad de las redes 5G y 6G, impulsada por la proliferación de dispositivos IoT y la demanda de servicios innovadores.

Network Digital Twin (NDT) emerge como una tecnología pivote, ofreciendo una representación virtual en tiempo real de la red física. Sus capacidades de análisis de rendimiento, emulación de escenarios "What-If" y control inteligente permiten a los operadores validar configuraciones y políticas sin riesgo, optimizar la planificación y reducir costos. Sin embargo, NDT enfrenta desafíos significativos, particularmente en la contextualización del Edge-Cloud Continuum (ECC) para múltiples *stakeholders* más allá de los operadores de red, la gestión de la masiva recopilación y procesamiento de datos, la seguridad y privacidad, la adaptación de modelos de IA/ML a la deriva de datos, y la necesidad de estandarización en el modelado y la validación de la confianza. La tensión entre la necesidad de una representación de alta fidelidad y la complejidad inherente de las redes dinámicas es una brecha crítica.

Zero Touch Management (ZTM) complementa a NDT al buscar la autonomía total de la red, habilitando capacidades de auto-configuración, auto-monitorización, auto-curación y auto-optimización sin intervención humana. ZTM es un imperativo estratégico para la agilidad y monetización de servicios en el ecosistema 5G/6G, permitiendo el despliegue y la gestión de servicios de forma rápida y eficiente. Sus principios de diseño, como la automatización de bucle cerrado y la gestión de servicios E2E entre dominios, son fundamentales para la escalabilidad y la "separación de preocupaciones" en entornos complejos.

La sinergia entre NDT y ZTM es la clave para la autonomía de la red. NDT actúa como el "cerebro" cognitivo y el "laboratorio de pruebas" de ZSM, proporcionando la inteligencia predictiva y la capacidad de validación sin riesgo que son esenciales para que ZSM opere de forma confiable. La integración de Inteligencia Artificial y Aprendizaje Automático (IA/ML) es el motor de esta sinergia, con el desarrollo de arquitecturas "AI-Native" y la aplicación de AutoML. Esta profunda integración subraya la necesidad de modelos de IA que no solo sean precisos y eficientes, sino también

adaptables a la deriva de datos y, crucialmente, explicables, para construir la confianza necesaria en la autonomía. La simulación y emulación, facilitadas por NDT, se convierten en componentes operativos esenciales para la prueba de fallos y la optimización continua en un entorno virtual.

Finalmente, la estandarización, impulsada por organismos como ETSI, IETF e ITU, es el puente crítico entre la investigación académica y la adopción industrial a gran escala. Sin estándares unificados, la interoperabilidad y la confianza en estas tecnologías se verían gravemente comprometidas. Los desafíos restantes, como la garantía de la seguridad y la privacidad en entornos altamente automatizados y ricos en datos, la validación de la confianza en los sistemas de IA y la gestión de la complejidad del Edge-Cloud Continuum, son áreas clave para la investigación y el desarrollo futuro. La superación de estos desafíos será fundamental para liberar todo el potencial transformador de NDT y ZTM en las redes de próxima generación, y que estos puedan ser aprovechados por los ISP de la región.

Si a esto le agregamos la capacidad técnica de los pequeños ISP, los retos ya mencionados son aún mayores para la adopción, aunque podrían ser los más beneficiados por estas tecnologías.

# 3 Sobre el uso de sistemas de IA basados en flujos (n8n) en la atención al cliente

El panorama de los Pequeños Proveedores de Servicios de Internet (PISPs o WISPs) se define por una competencia feroz y una dependencia directa de la excelencia en el servicio al cliente. En este entorno, la capacidad de respuesta y la eficiencia operativa dejan de ser ventajas y se convierten en requisitos de supervivencia. La gestión técnica y operativa de un PISP debe buscar herramientas que neutralicen las desventajas inherentes a su escala.

## 3.1 Contexto Competitivo: La Lucha del Pequeño ISP contra las Desventajas de Escala

Los pequeños operadores enfrentan una desventaja estructural significativa en la economía del tráfico de Internet. El análisis de costos revela que mientras los grandes operadores pueden

"cachear" en CDN’s aproximadamente el 58% del tráfico de servicios populares (como Google, Facebook o Netflix), los pequeños ISPs deben pagar por el total de su canal de datos. Esta disparidad genera un sobrecosto operativo que se acerca al 60% del valor de acceso al producto que proveen, lo que exige una búsqueda implacable de eficiencia en cada otra área del negocio para preservar la rentabilidad.

A pesar de esta presión financiera, la supervivencia y el crecimiento de los ISPs se debe a su diferenciador más potente: el servicio al cliente. Los pequeños proveedores han logrado crecer porque "Respetan, valoran y cuidan a sus clientes". Su ventaja competitiva se basa en la cercanía, el conocimiento profundo de sus comunidades y la capacidad de ofrecer una respuesta y atención inmediata. Se ha observado que, tras una falla, un propietario de un ISP puede estar reparando un inconveniente en la finca de un cliente en menos de dos horas, marcando un punto de inflexión frente a la burocracia de los grandes operadores.

No obstante, esta ventaja se ve constantemente amenazada por los puntos de dolor que provocan la insatisfacción y la alta tasa de abandono (*churn*) en la industria. Los clientes priorizan consistentemente la fiabilidad y consistencia del servicio, la velocidad de Internet prometida y la claridad en el precio y la facturación. Un factor crítico de frustración es el tiempo de resolución de problemas, exacerbado por el fenómeno de "echar la culpa" entre el proveedor, el equipo del cliente y la infraestructura física. La facilidad para cambiar de proveedor significa que los ISPs que no modernicen su enfoque de interacción con el cliente perderán rápidamente usuarios. El uso de herramientas de atención al cliente basadas en flujos low code de IA, como es el caso de n8n, Zapier, Activepieces, UiPath, o Shuffle, por mencionar solo algunas, puede ayudar a mejorar ese diferenciador ya mencionado. A continuación se hace una revisión de las ventajas y posibles aplicaciones de dichas tecnologías, usando como referencia n8n, por ser tal vez una de las más populares, aunque es importante mencionar que tiene restricciones cuando los flujos se vuelven complejos y grandes.

## 3.2 Introducción a n8n: Low-Code Estratégico para Pequeños ISPs

n8n emerge como la plataforma de automatización de flujos de trabajo más adecuada para el entorno técnico y financiero del pequeño ISP. Se define como una herramienta *low-code/no-code* que ofrece la precisión del código con la velocidad de arrastrar y soltar.

Una distinción crucial de n8n es su flexibilidad técnica. A diferencia de las plataformas puramente *no-code*, n8n está diseñado para equipos técnicos, permitiendo la inclusión de lógica personalizada mediante la escritura de código JavaScript o Python, y la incorporación de librerías (npm o Python). Esta capacidad de codificación es vital para interactuar con sistemas propietarios y equipos de red (como Mikrotik) cuya documentación de API requiere implementaciones específicas.

Desde la perspectiva de la infraestructura, n8n ofrece la opción de auto hospedaje (*self-hosted*)

vía Docker o Kubernetes. Para un ISP que gestiona datos de clientes y controla infraestructura de red, la opción de auto hospedaje garantiza el control total sobre los datos, la seguridad y el cumplimiento de regulaciones de privacidad (como GDPR o CCPA), un factor esencial en la industria de telecomunicaciones.

### 3.2.1 La Ventaja Financiera del Diagnóstico Complejo

El modelo de precios de n8n está basado en la **ejecución de flujo**, no en el número de pasos o tareas, lo que proporciona costos predecibles y fomenta la creación de lógica robusta. En contraste con alternativas donde cada paso dentro de un flujo se factura como una "tarea", en n8n, un flujo de diagnóstico exhaustivo que involucre 200 pasos de chequeos de sistemas y lógica compleja cuenta como una única ejecución.

Esta estructura tarifaria permite a la gerencia técnica diseñar flujos de diagnóstico preventivo y reactivo extremadamente detallados, sin temor a una factura masiva. Un diagnóstico automatizado que ejecuta 15 o 20 interacciones (chequeo de facturación, ping a la CPE, consulta a Mikrotik, actualización del *ticket*) cuesta lo mismo que una automatización de dos pasos. Esto es un factor determinante, ya que el costo por hora de soporte técnico especializado para la reparación de averías puede oscilar entre USD $75 y $250, o incluso alcanzar los USD $300 por hora en tarifas de respuesta de emergencia. Al incentivar flujos de diagnóstico exhaustivos y automáticos, se minimiza la necesidad de desplazar personal costoso para revisiones preliminares.

### 3.2.2 La Paradoja de la Automatización Personalizada

La adopción de la automatización en el servicio al cliente por parte de un ISP debe ser vista como un mecanismo para potenciar, y no reemplazar, su principal ventaja competitiva: la atención personalizada. Existe la noción de que la automatización se opone a la personalización, pero la realidad operativa de un ISP en crecimiento requiere ambos enfoques[27].

La estrategia consiste en utilizar flujos low code para **automatizar los problemas simples y masivos** (ej. preguntas de facturación, solicitud de *reseteo* de *password*, o chequeos de conectividad Tier 0). Al delegar estas tareas repetitivas y de alto volumen, se reduce el error humano y se acelera el tiempo de respuesta operativo. Esto, a su vez, libera al personal humano más capacitado para concentrarse en los problemas menos frecuentes y más complejos, como el diagnóstico de fallas críticas en la red o las conversaciones proactivas de retención de clientes. De esta manera, las herramientas low code/No code permiten al ISP ganar eficiencia operativa y, simultáneamente, elevar la calidad de la atención humana en los momentos más críticos para la satisfacción del cliente.

## 3.3 Arquitectura de Solución y Cimientos Técnicos

# con herramientas low code

La implementación de n8n como plataforma central de automatización requiere una arquitectura sólida que garantice control, escalabilidad y una integración profunda con los sistemas de red existentes del ISP.

## 3.3.1 Modelo de Despliegue Estratégico: Control y Escalabilidad

Para la mayoría de los ISPs que requieren integrar su infraestructura de red, el modelo de **autohospedaje** (*Self-Hosted*) es la opción estratégica. La implementación se puede realizar rápidamente utilizando contenedores Docker o K8s. Aunque el software principal es de código abierto ($0 de licencia), se debe presupuestar la infraestructura subyacente. Los costos de infraestructura, mantenimiento y seguridad para un entorno de producción básico suelen superar los USD$200 al mes, pero esta inversión es mínima en comparación con el control total de los datos y la capacidad de interconexión con redes privadas.

Para garantizar la fiabilidad en entornos de misión crítica, como los sistemas de facturación y suspensión de servicio, se recomienda la configuración de **Queue Mode** (Modo Cola). Este modo desacopla la recepción de la solicitud de su ejecución, permitiendo que múltiples *workers* procesen flujos en paralelo. Esta resiliencia es vital para manejar picos de solicitudes, como los que ocurren después de una caída masiva de servicio o durante un ciclo de suspensión por mora. Adicionalmente, n8n soporta prácticas de desarrollo profesional, incluyendo la separación de ambientes (Desarrollo, Staging y Producción) y el control de versiones mediante GitOps, lo cual asegura que las modificaciones y pruebas de nuevos flujos no comprometan la operación en vivo.

## 3.3.2 Centralización de Canales de Comunicación (Unified Inbox)

La fragmentación de los canales de soporte (email, teléfono, redes sociales) es un obstáculo importante para reducir los Tiempos Medios de Respuesta (MTTR o Mean Time to Repair). n8n resuelve esto mediante la creación de un *Unified Inbox* (bandeja de entrada unificada) inteligente que puede reducir los tiempos de respuesta hasta en un 80%.

- **Integración Multicanal:** n8n utiliza triggers (disparadores) de eventos para consolidar la atención desde fuentes como el monitoreo de buzones IMAP, *Webhooks* para formularios web o aplicaciones de chat, y nodos dedicados o HTTP Requests para plataformas de mensajería populares en América Latina, como WhatsApp Business Cloud y Telegram.
- **Triage Inteligente impulsado por IA:** Una vez que el mensaje del cliente ingresa al flujo de n8n, se activa un Agente de IA (utilizando integraciones con modelos como Gemini o GPT). Este agente es responsable de:
    - **Clasificación Automática:** Categorizar la solicitud en temas como 'Facturación', 'Falla de Conexión', 'Soporte Técnico' o 'Reclamo'.
    - **Asignación de Prioridad y Sentimiento:** Determinar la urgencia y el

sentimiento del cliente, escalando inmediatamente los casos de clientes frustrados o VIP.
- **Extracción de Datos Clave:** Recopilar automáticamente la información necesaria (nombre, email, descripción del problema) para estructurar el ticket.

Esta inteligencia asegura que el *ticket* de soporte (por ejemplo, en Jira, Trello, o un sistema de *ticketing* integrado en WHMCS, cPanel o herramientas similares) llegue al agente humano ya clasificado, etiquetado y priorizado, eliminando la latencia del triage manual.

## 3.3.3 Integración con Sistemas Críticos del ISP

El verdadero valor de n8n para el ISP radica en su capacidad para orquestar acciones entre sistemas de gestión y la infraestructura de red.

### 3.3.3.1 Integración con Mikrotik y APIs de Red

Los equipos Mikrotik son omnipresentes en la infraestructura de los ISPs en Latinoamérica. n8n no solo es capaz de integrarse con estos dispositivos, sino que simplifica la interacción. Si bien la API de RouterOS es potente, su dominio requiere un conocimiento especializado. n8n reduce esta curva de aprendizaje al utilizar el nodo genérico

**HTTP Request** para interactuar directamente con la API REST de Mikrotik[28].
Para realizar acciones críticas como la suspensión o reactivación de un usuario, el ISP encapsula la lógica compleja en scripts predefinidos directamente en el router. El flujo n8n simplemente ejecuta el script deseado enviando una solicitud POST a la URL /rest/system/script/run. Este enfoque convierte la compleja tarea de desarrollo de *full-stack* para la gestión de red en un paso visual dentro de un flujo Low-Code.

### 3.3.3.2 Integración con Sistemas de Billing (WHMCS, WISECP, MikroWisp, WisPro)

Los sistemas de gestión y facturación (como WHMCS, MikroWisp, Wispro o WISECP) son los disparadores naturales para los flujos transaccionales y de soporte. n8n puede ser configurado como un *backend* de API, recibiendo comandos de estos sistemas y ejecutando acciones automatizadas. Por ejemplo, un *webhook* de WHMCS que notifica una factura vencida puede disparar el flujo de morosidad. De manera inversa, n8n puede utilizar las APIs de estos sistemas (ej. OpenTicket API de WHMCS) para crear tickets estructurados o actualizar el estado de la cuenta.

## 3.3.4 La Estrategia de Cobro en LATAM

La gestión eficiente de la morosidad impacta directamente la liquidez del ISP. Las pasarelas de pago en América Latina (como PayU o Mercado Pago) son esenciales porque soportan métodos locales como PSE y ofrecen APIs robustas. Un flujo n8n puede integrarse con estas APIs para:

1. **Generar Enlaces de Pago Personalizados:** Integrar los datos del cliente y la deuda desde el sistema de *billing* para generar un enlace de pago único.
2. **Notificación Proactiva:** Enviar este enlace inmediatamente al cliente a través de su canal preferido (WhatsApp/Telegram).
3. **Activación de Servicio Instantánea:** El *webhook* de confirmación de pago de la pasarela de pago dispara el flujo de reactivación en n8n, el cual, en segundos, ejecuta el *script* de habilitación en el Mikrotik o en la plataforma de gestión o el sistema AAA.

Esta orquestación automatiza completamente el ciclo de cobro y reactivación, reduciendo la morosidad y eliminando la intervención humana en un proceso repetitivo y de alto volumen. En el apartado siguiente, se muestran algunos ejemplos de flujos críticos que podrían ser desplegados con n8n.

## 3.4 Algunos Flujos de Automatización Crítica en la Atención al Cliente (Use Cases)

Los siguientes casos de uso representan las automatizaciones de mayor impacto operativo y financiero que un ISP podría implementar con n8n.[29]

### 3.4.1 Flujo Crítico 1: Gestión Automatizada de Morosidad (Suspender y Reactivar)

Este es el flujo de Retorno de Inversión (ROI) más inmediato para un ISP, ya que asegura la recaudación y minimiza el riesgo financiero asociado a la falta de pago.

1. **Trigger (Disparador):** El flujo se inicia con un evento de "Pago Vencido" enviado por el sistema de Billing (WHMCS/WISECP) a un *Webhook* de n8n. El evento debe transportar la identificación del cliente y el nombre de usuario asociado en Mikrotik.
2. **Notificación Personalizada y Preventiva:** n8n utiliza un nodo de mensajería (ej. WhatsApp Business Cloud o Telegram) para enviar una notificación proactiva. Esta notificación incluye el monto adeudado y el enlace de pago personalizado generado a través de la API de la pasarela de pago local (ej. PayU/PSE, en el caso colombiano).
3. **Lógica Condicional de Suspensión:** Se implementa un nodo de espera y una bifurcación (Branching). Si el pago no se recibe después de un período definido (ej. 24 o 48 horas, según la política), el flujo avanza a la suspensión.
4. **Ejecución de Suspensión (Mikrotik API):** Se utiliza el nodo **HTTP Request** para la interacción directa con el router de borde. La acción es una solicitud POST a la URL de ejecución de *scripts* en RouterOS: https://[IP_Mikrotik]/rest/system/script/run. El *payload* incluye el nombre del script de suspensión (disable-user-script) y los argumentos necesarios (el ID del cliente).
5. **Reactivación Automática y Unificada:** Un segundo flujo o rama se mantiene a la escucha del *Webhook* de "Pago Exitoso" de la pasarela de pago. Al recibir la confirmación, n8n ejecuta un script de reactivación similar en Mikrotik (ej.

enable-user-script), restaurando el servicio en cuestión de segundos, mejorando dramáticamente la experiencia del cliente y la eficiencia del cobro.

### 3.4.2 Flujo Crítico 2: Diagnóstico Inicial Inteligente y Respuesta Inmediata (Tier 0)

Este flujo se enfoca en resolver las quejas de servicio más comunes (el 80% de las incidencias) sin necesidad de intervención humana especializada.

1. **Trigger:** Recepción de un ticket de soporte a través de cualquier canal unificado (ej. mensaje de Telegram con el texto "Internet lento").
2. **Pre-Triage y Análisis de IA:** El Agente de IA clasifica la queja como "Técnica - Conectividad" y realiza un Análisis de Sentimiento. Si el cliente está "Frustrado", la prioridad aumenta automáticamente.
3. **Diagnóstico Automatizado (Checklist de Salud):** El flujo consulta la base de datos de clientes para identificar la CPE y utiliza el nodo **HTTP Request** para ejecutar un chequeo de estado remoto (ej. verificar la latencia o el registro en la OLT/Mikrotik).
4. **Acción Correctiva de Nivel Cero:**
    - Si el diagnóstico remoto indica una solución sencilla (ej. reinicio de *hardware* o congestión leve), n8n envía un comando (vía API/SSH) para forzar un reinicio remoto de la CPE.
    - **Respuesta al Cliente:** n8n responde automáticamente al canal de origen (WhatsApp/Telegram) con una respuesta personalizada: "Hemos detectado un posible problema en su equipo y hemos ejecutado un reinicio remoto. Si la falla persiste en 10 minutos, se escalará un ticket de alta prioridad a un técnico Nivel 1.
5. **Escalamiento Inteligente:** Si el diagnóstico falla o el problema persiste, n8n crea un ticket categorizado en el sistema de *ticketing* e inmediatamente notifica al equipo técnico humano vía Slack o Telegram, con toda la información de diagnóstico ya adjunta.

### 3.4.3 Flujo Crítico 3: Captura de Feedback y Métrica de Retención

Dado que la retención es uno de los pilares de la estrategia de los ISP, n8n ayuda a automatizar la medición de la satisfacción y el seguimiento proactivo de los usuarios.

1. **Trigger:** El flujo se activa al cierre de un ticket de soporte o 24 horas después de la reactivación automática del servicio (Flujo 1).
2. **Encuesta y Recolección de Datos:** n8n envía automáticamente una encuesta breve (NPS o CSAT) a través de un enlace de *webhook*.
3. **Análisis de IA y Escalamiento:** El flujo utiliza nodos de IA para analizar las respuestas de texto libre, extrayendo el sentimiento y las tendencias de mejora. Si el resultado es un NPS bajo o el sentimiento es marcadamente negativo, n8n crea una alerta o una tarea de *follow-up* de "Retención Activa" dirigida al gerente de servicio, asegurando que ningún cliente insatisfecho pase desapercibido.

En la Tabla 1 se muestra un resumen de los flujos descritoes antes, con sus paraémtros clave para la configuración.

*Tabla 1Matriz de Automatización de Soporte Crítico para ISPs*

| Caso de Uso (Punto de Dolor) | Objetivo de UX/Negocio | Trigger (Disparador n8n) | Integraciones Clave (API) | Técnica de n8n Central |
|---|---|---|---|---|
| **Suspensión Automática por Mora** | Reducir el riesgo de *Churn* y pérdidas por impago. | Webhook (WHMCS/WISECP) o Time Trigger.[27] | Mikrotik API [26], Billing API. | HTTP POST para ejecutar script de desactivación de usuario /rest/system/script/run.[26] |
| **Diagnóstico Inicial Inteligente** | Reducir el Tiempo Medio de Respuesta (MTTR) y derivar menos llamadas al Nivel 1. | Mensajería (WhatsApp/Telegram) o Email.[18] | AI Agent (Gemini/OpenAI) [20], Mikrotik (Status Check). | Análisis de Lenguaje Natural (NLP) + Consulta HTTP de Estado de Servicio. |
| **Creación de Tickets/Triage** | Mejorar la eficiencia del agente humano al reducir el tiempo de clasificación. | Recepción de Email/Mensaje (IMAP, Webhook).[16] | AI Agent [21], Sistema de Ticketing (Jira/Trello/WHMCS).[22] | Clasificación semántica, Asignación de Prioridad y Notificación en tiempo real.[16] |
| **Notificación de Pago y Reactivación** | Automatizar el ciclo de cobro y restaurar el servicio en segundos. | Webhook (Pasarela de Pago: PayU/Mercado Pago).[29] | Mikrotik API, Pasarela de Pago API. | Flujo Bifurcado: POST para suspensión; Webhook de respuesta para reactivación. |

## 3.5 Operación, Resiliencia y Optimización de la Solución

Dada la naturaleza crítica de los flujos del ISP, que gestionan los ingresos (cobranza) y la provisión del servicio (Mikrotik), la resiliencia operativa de n8n es un requisito no negociable para el ISP. Un fallo en el flujo de reactivación, por ejemplo, puede resultar en la pérdida de un cliente, mientras que un fallo en la suspensión significa una pérdida directa de ingresos.

### 3.5.1 Estrategia de Manejo de Errores Críticos (Professional Error Handling)

La gestión de errores debe ser profesional y centralizada. n8n y las herramientas similares permiten configurar un **Flujo Centralizado de Errores** (*Error Workflow*) que se activa automáticamente cuando cualquier otro flujo de producción falla.

El Error Workflow funciona como una póliza de seguro operacional. Su propósito principal es notificar al equipo técnico en tiempo real sobre la naturaleza exacta del fallo. Esto se logra capturando la información detallada del error (datos que lo causaron, el nodo fallido y el ID de ejecución). Inmediatamente, el flujo envía alertas de alta prioridad a canales dedicados (SMS, Slack, o Telegram, utilizando codificación de color para prioridad).

La capacidad de n8n de proporcionar la URL de la ejecución que falló es fundamental, ya que permite al técnico intervenir en el flujo fallido en minutos para Re ejecutar pasos o corregir datos, salvando la transacción (cobro o reactivación) y minimizando el impacto en la relación con el cliente. Además, se recomienda utilizar el nodo  Stop And Error en los flujos principales (como la suspensión) en caso de que se detecte una anomalía controlada, forzando la activación del Error Workflow y evitando que el flujo principal continúe con datos erróneos.

### 3.5.2 Colaboración y DevOps para la Automatización

El ISP debe gestionar su automatización de n8n como si fuera código de infraestructura para garantizar la continuidad del negocio. El autohospedaje facilita la implementación de las mejores prácticas de DevOps.

El **Control de Versiones (GitOps)** es esencial. Los flujos de n8n se almacenan como archivos JSON, que deben ser versionados en un repositorio Git. Esto permite que el equipo revierta rápidamente cualquier cambio problemático, facilita la colaboración entre técnicos y asegura un registro inmutable de la lógica de negocio. Para el mantenimiento a largo plazo, el equipo debe seguir un ciclo proactivo que incluya la revisión periódica de flujos, la documentación detallada de la lógica de negocio y la actualización inmediata de nodos y credenciales ante cualquier cambio en las APIs de Mikrotik o WHMCS.

La visualización de procesos complejos mediante flujos *low-code o no-code* en n8n reduce la curva de aprendizaje de las operaciones críticas. Los ISPs a menudo operan con equipos técnicos reducidos donde el conocimiento puede estar concentrado. Al externalizar la lógica compleja de Mikrotik o Billing en un diagrama de flujo n8n, se facilita la transferencia de conocimiento técnico.[30]

El personal de soporte o incluso administradores menos familiarizados con la programación de redes pueden seguir y modificar la lógica de negocio visualmente, lo que maximiza los resultados del equipo técnico existente.

### 3.5.3 Medición y Mejora Continua (KPIs Clave)

El éxito de la plataforma de automatización se mide a través del impacto en las métricas de negocio.
La implementación de los flujos de n8n impacta directamente en los KPIs de atención al cliente y retención:

- **Tiempo Medio de Respuesta (MTTR) y Resolución del Primer Contacto (FCR):** El triage automatizado y la resolución de Nivel 0 reducen drásticamente el tiempo que el cliente espera una respuesta humana. Los flujos de autodiagnóstico aumentan la FCR, resolviendo el problema en la primera interacción.
- **Valor de Vida del Cliente (CLV) y Tasa de Abandono (*Churn Rate*):** Al mejorar la calidad del servicio (a través de la velocidad de respuesta y la atención personalizada delegada) y al asegurar notificaciones proactivas de cobro/servicio, la retención mejora significativamente.
- **Métricas de Satisfacción (NPS/CSAT):** Utilizar n8n para rastrear automáticamente las puntuaciones de satisfacción en múltiples plataformas y realizar análisis de sentimiento con IA permite una mejora continua y basada en datos de la experiencia del cliente.

## 3.6 Análisis de Costo-Beneficio y Roadmap de Implementación

La decisión de adoptar n8n se justifica por una ventaja de costos estructurales y un alto retorno de la inversión derivado de la eficiencia operativa y la mejora en la retención[31].

La principal justificación financiera para un ISP que maneja lógica de red compleja es el modelo de ejecución de n8n.

El plan Cloud de n8n comienza en $20 USD por mes e incluye 2,500 ejecuciones de flujo. A diferencia de otras plataformas que cobran por cada paso o tarea (lo cual penalizaría severamente un diagnóstico de 100+ pasos) n8n permite al ISP construir flujos de lógica detallada sin incrementar el costo más allá del precio base por ejecución.

Para el modelo **Self-Hosted** (el recomendado), el costo del software es nulo, pero la empresa debe considerar los costos ocultos de infraestructura, mantenimiento, seguridad y la necesidad de contar con experiencia en DevOps. Sin embargo, esta inversión está compensada por el control total sobre los datos, la privacidad (crucial para el sector) y la capacidad de interactuar libremente con APIs de red privadas, como las de Mikrotik, sin pasar por servidores de terceros. La Tabla 2 muestra una comparación de costos entre n8n y otras herramientas similares.

*Tabla 2. Análisis Comparativo de Costos de Automatización*

| Plataforma | Modelo de Precios Principal | Ventaja Clave para PISPs | Consideraciones de Costo Oculto | Citas Relevantes |
|---|---|---|---|---|
| **n8n (Cloud)** | Ejecución-basada (€20 / 2.5K | Permite lógica compleja y | Costos de ejecución crecen con el | [8] |

| | | | | |
|---|---|---|---|---|
| | ejecuciones) | multi-paso (ej. diagnóstico) sin penalización por paso. Costos predecibles.[8] | volumen de tráfico.[38] | |
| **n8n (Self-Hosted )** | Open Source (Licencia Gratuita) | Control total sobre la infraestructura y datos. Ideal para APIs propietarias (Mikrotik) y cumplimiento.[6] | Infraestructura, mantenimiento, seguridad y soporte técnico especializado.[9] | [6] |
| **Alternativas (Ej. Make, Zapier)** | Por tarea/operaciones | Mayor simplicidad para usuarios no técnicos. | Alto costo para flujos complejos o multi-paso; límites en el uso de código y la capacidad de interactuar con sistemas de red internos.[9] | [9] |

### 3.6.1 Retorno de la Inversión (ROI) en el PISP

El ROI se materializa a través de dos vectores principales:

1. **Ahorro Operativo Directo:** La automatización de tareas repetitivas puede liberar horas semanales por empleado. Si un ISP automatiza solo el 50% de las suspensiones, reactivaciones y diagnósticos iniciales, el ahorro de costos por hora-hombre técnica, que puede ser de USD $75 a $250 por hora, supera rápidamente la inversión en infraestructura y *hosting* de n8n.
2. **Aumento de la Retención y Liquidez:** Al automatizar el ciclo de cobranza y garantizar la restauración instantánea del servicio tras el pago, se mejora la liquidez y se reduce el *churn* relacionado con fallas operativas o morosidad.[32]

### 3.6.2 Roadmap Sugerido para la Implementación (Enfoque Prescriptivo)

Una implementación exitosa de una plataforma de automatización debe seguir fases estructuradas de migración y modernización para garantizar una transición fluida y sin interrupciones en el servicio, tal como se describe a continuación.[33]

**Fase 1: Evaluación y Diseño (2-4 semanas)**
El primer paso es un diagnóstico exhaustivo de los procesos internos. Se deben identificar los cuellos de botella operativos y las tareas más repetitivas del soporte. La decisión crucial en esta fase es la arquitectura: si se opta por el *Self-Hosted*, se debe instalar inmediatamente el entorno inicial (Docker o K8s) y establecer los parámetros de red y seguridad. El equipo debe mapear los tres flujos de mayor impacto operativo (Morosidad, Triage Inteligente, Reactivación)

para el piloto inicial.

**Fase 2: Movilización y Desarrollo Piloto (4-8 semanas)**

Esta fase se centra en establecer la conectividad fundamental.

1. **Integración Core:** Establecer credenciales API y probar la conectividad con Mikrotik y el sistema de Billing .
2. **Desarrollo Piloto:** Construir los flujos críticos (Morosidad y Triage) en un ambiente aislado de Dev/Staging.
3. **Resiliencia Operativa:** Diseñar e implementar el **Flujo Centralizado de Errores** (Error Workflow) para el piloto, configurando las notificaciones de alerta. Esta capa de seguridad es fundamental antes de cualquier despliegue en producción.

**Fase 3: Migración, Pruebas y Producción (4-6 semanas)**

Antes de la activación masiva, es esencial realizar pruebas rigurosas para asegurar que el sistema cumpla con los requisitos de funcionalidad y rendimiento.

1. **Pruebas de Carga:** Simular un alto volumen de ejecuciones (ej. 100 suspensiones/reactivaciones simultáneas) para validar la configuración de Modo Cola (*Queue Mode*) y la resiliencia.
2. **Activación:** Desplegar los flujos aprobados al ambiente de Production utilizando buenas prácticas de GitOps[3].
3. **Monitoreo y Optimización:** Monitorear activamente los KPIs de servicio (MTTR, FCR, Tasa de Abandono) para validar el ROI y realizar ajustes finos a la lógica de negocio y los modelos de IA.

# 3.7 Conclusiones de la sección

La automatización de flujos de trabajo con n8n ofrece al Pequeño Proveedor de Servicios de Internet una solución estratégica para mitigar sus desventajas de escala y potenciar su principal ventaja competitiva.

La arquitectura *low-code* de n8n, con su capacidad de incorporar código personalizado y su modelo de precios basado en la ejecución, es particularmente adecuada para los ISPs que requieren integraciones profundas y complejas con sistemas de red como Mikrotik y APIs de pasarelas de pago. Esta flexibilidad permite crear flujos de diagnóstico complejos y robustos (Tier 0) que resuelven problemas repetitivos y reducen los costosos desplazamientos de soporte técnico.

La integración de Agentes de IA en el triage de soporte garantiza que las consultas de los clientes sean clasificadas, priorizadas y dirigidas con una eficiencia que iguala o supera a los grandes operadores. Al automatizar lo masivo y lo mundano (como la suspensión automática por mora y la reactivación instantánea), el ISP puede liberar a su personal altamente capacitado. Estos técnicos pueden entonces enfocarse en el elemento que tradicionalmente asegura la retención: la atención humana, personalizada y de alta calidad para los problemas más críticos y las interacciones de retención más sensibles. En resumen, n8n transforma la eficiencia operativa en una estrategia de atención al cliente superior.

# 4 Encuesta

Se ejecutó una encuesta entre ISP's donde se preguntaba por diversos aspectos relacionados con el uso de IA en la gestión de redes, así como acerca de ciertas prácticas por parte de los ISP. La encuesta fue enviada a cerca de 200 operadores, y se obtuvieron 10 respuestas.

De las respuestas obtenidas, se puede decir que hay un interés por el uso de IA para mejorar la atención al cliente y mejorar la operación de la red. Al hacer la pregunta abierta ¿Cómo le gustaría usar la IA para la operación de su red?, las respuestas se orientan hacia la identificación automática de fallas y la gestión completa entre lo administrativo y la detección automática de fallas, de forma que se mejore la eficiencia con el mismo o menos personal del actual.

Ante la pregunta sobre el posible uso de gemelos digitales para mejorar la gestión de red, un 40% respondió que le parece que esta tecnología puede ayudar a mejorar la gestión, un 40% opina que no serviría y un 20% no sabe.

Si existiera una plataforma basada en el concepto de "Gemelos Digitales", solo el 20% respondió afirmativamente, otro 20% respondió que no, y el resto se encuentra entre la opción de tal vez o "necesito pensarlo". Se recibieron algunas sugerencias generales, donde los encuestados esperan que este tipo de herramientas basadas en IA permitan entregar información actualizada y en tiempo real.

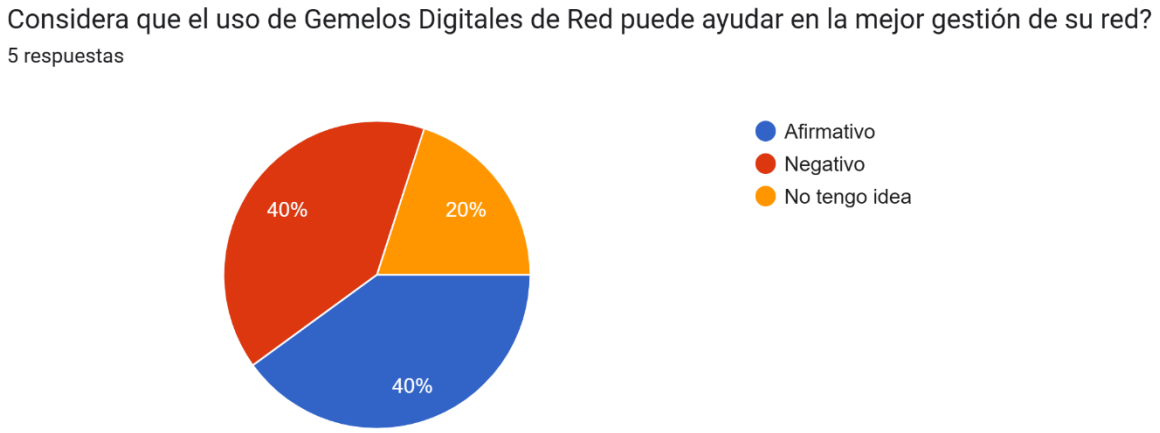


*Figura 1 Gráfico de respuesta a la pregunta sobre el uso de gemelos digitales*

A la pregunta acerca de si usan algún software de gestión de red, el 100% respondió afirmativamente, sin embargo, el 60% utiliza herramientas diferentes a las mencionadas en la pregunta. Esto nos deja con Mikrowisp y Zabbix, además de otras herramientas como Wispro,

Integra y Dude. Es importante mencionar que Dude es otra herramienta utilizada por Mikrotik, lo que de alguna forma la ubica cerca a Mikrowisp en términos de a qué fabricante está orientada principalmente.

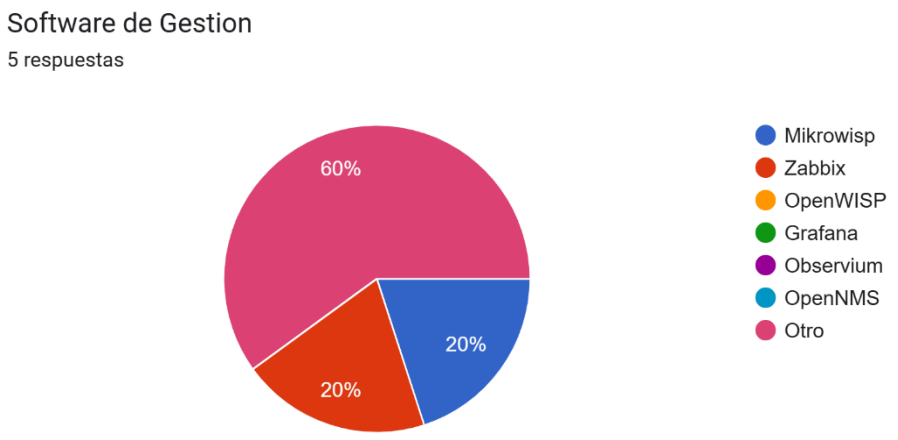


*Figura 2. Respuestas acerca de si usan o no software de gestión de red*

A continuación se resumen algunas de las funcionalidades de las herramientas mencionadas en la encuesta.. **The Dude** y **Zabbix** son herramientas de **monitoreo de red (NMS)**, enfocadas en la visibilidad del estado y rendimiento de la infraestructura. The **Dude** tiene una integración nativa y más profunda con **MikroTik**, mientras que Zabbix es una solución empresarial de código abierto más amplia y personalizable.

**Wispro** y **Mikrowisp** son plataformas de **Gestión de Proveedores de Internet (ISP/WISP)**. Su principal fortaleza es la **automatización de procesos comerciales y operativos** (facturación, corte/reconexión de clientes, soporte) con una fuerte integración con *routers* MikroTik.

**Integra** , es una herramienta desarrollada por una empresa colombiana, para la gestión de ISP. La plataforma que ofrecen permite centralizar y optimizar todos los procesos del ISP con una sola herramienta.

La siguiente tabla (Tabla 3) resume las características de las herramientas mencionadas, de acuerdo a la lista de sitios donde se encontró información.

*Tabla 3. Resumen de características de las herramientas de gestión mencionadas en la encuesta.*

| Herramienta | Tipo principal de Herramienta | Características y Funcionalidades Clave |
|---|---|---|
| **The Dude** | Sistema de Monitoreo de Red (NMS) (de MikroTik) | Mapeo y Descubrimiento Automático: Genera automáticamente un diagrama visual de la topología de la red, detectando dispositivos de cualquier tipo o marca. Monitoreo: Controla servicios (SNMP, ICMP, DNS, TCP, etc.), rendimiento, uso de CPU y tráfico. |

| | | |
|---|---|---|
| | | Alertas y Notificaciones: Ofrece múltiples métodos de notificación (correo, API para SMS/WhatsApp/Push) cuando hay problemas. Gestión MikroTik: Permite la gestión individual o simultánea de dispositivos MikroTik. |
| **Zabbix** | Sistema de Monitoreo Empresarial de Redes, Servicios y Aplicaciones (Open Source) | Recolección de Métricas: Recopila datos de alta intensidad de dispositivos de red, servicios en la nube, máquinas virtuales, bases de datos y aplicaciones (soporte para SNMP, Monitoreo Web, Java, IPMI, SSH/Telnet). Alertas y Acciones: Envía notificaciones escalables y programables, y puede ejecutar scripts remotos para la corrección automática de problemas. Visualización: Dashboards personalizados, gráficos dinámicos, mapas de infraestructura y reportes programados en PDF. Análisis de Servicios: Define y monitorea niveles de SLA, con análisis de impacto. |
| **Wispro** | Software de Gestión y Administración para Proveedores de Internet (ISP/WISP) | Gestión Comercial y Operativa: Administración de clientes, planes, facturación automática (con facturación electrónica en varios países de Latam), pasarelas de pago y cortes automáticos por morosidad. Control de Red: Soporte para control de ancho de banda en MikroTik (Simple Queues, PPPoE, Hotspot, PCQ) y gestión OLT-ONU. Soporte y Movilidad: Sistema de ticketing de soporte, portal de clientes (Alerta Internet) para pagos y reportes, y aplicación móvil para técnicos (órdenes de instalación y gestión en campo). Geolocalización: Ubica clientes, routers y traza rutas en Google Maps. |
| **Mikrowisp** | Plataforma de Gestión y Automatización para ISPs/WISPs (con enfoque en MikroTik) | Automatización Operativa: Alta, suspensión y reconexión automática de usuarios (PPPoE, Hotspot, Amarre IP, PCQ) vía API con MikroTik. Facturación y Cobranza: Generación de facturas automáticas, corte automático por falta de pago y notificaciones de pago (correo, SMS, aviso en pantalla). Gestión de Clientes: Portal del cliente para historial, pagos y tickets de soporte. Soporte y Movilidad: Sistema de ticketing, acceso multiusuario y aplicación móvil para administradores y técnicos. Monitoreo Básico: Muestra el estado Online/Offline de emisores y clientes (SNMP/ICMP). |
| **Integra** | Software de Gestión de ISP ( | Integra Colombia Software es una empresa dedicada a ofrecer soluciones de software para la gestión integral de empresas de telecomunicaciones en una sola plataforma. |

Otra pregunta de la encuesta estaba orientada a indagar sobre el tipo de esquema de gestión de direcciones IP, obteniendo un 80% de respuestas con IP fijas y solamente un 20% que utiliza DHCP o algún mecanismo de asignación dinámica (SLAAC en el caso de quienes ya han

migrado a IPv6). Recientemente, se mencionó en un blog de redes, el hecho de que esta es una discusión existente aún en el medio de los pequeños ISP.

Se preguntó también si se tiene un servidor dedicado en el NOC, a lo que el 60% respondió que sí y el 40% no lo tiene.

Adicionalmente, a la pregunta acerca del uso de software de registro o cancelación de usuarios, el 60% respondió que no, por lo que se podría suponer que este manejo se hace directamente desde el router, lo que es una práctica común. Como complemento a la pregunta anterior, se preguntó la herramienta que utilizan, y dos respondieron

La siguiente pregunta está orientada a indagar acerca de los mecanismos para atender solicitudes de los clientes, el 80% de los ISP tienen algún sistema de manejo de solicitudes o PQR, el 89% usan también mecanismos como WhatsApp o llamadas telefónicas. Al indagar por el tipo de sistema de manejo de tickets, se encontraron cinco diferentes herramientas, incluidos desarrollos propios. Las herramientas utilizadas son: Vtiger, Integra, **Wispro** (que también es un sistema de gestión de red fuertemente integrado con MikroTik) y Zohodesk. Todos manifiestan reportar los procesos de reclamos al regulador nacional.

La siguiente parte de la encuesta se enfoca en indagar acerca del uso de herramientas de IA ampliamente conocidas, de tipo LLM, como ChatGPT, Gemini, Perplexity, entre otras. EL total de las respuestas fueron afirmativas, al decir que han usado este tipo de herramientas. El 60% manifiesta usarlas con frecuencia, mientras que el 40% restante manifiesta usarlas poco.

Acerca del interés de contar con herramientas de atención al cliente basadas en IA, como pueden ser los chatbots, los encuestados respondieron un alto inter'es (4 y 5, donde 5 es "me interesa mucho").

Sobre el uso de herramientas de IA para detección de fallas o para la predicción del uso del ancho de banda del canal, el 80% está muy interesado en usarlas para predicción de ancho de banda (5), mientras que para detección de fallas, el 60% marcó 4 de 5 y el 20% marcó 5. Esto indica que hay más interés en el uso de herramientas de IA para predicción de tráfico, existiendo también un alto interés en la detección de fallas. Al indagar sobre el uso de IA para PREDICCION de fallas en la red, la distribución fue la misma que para la pregunta sobre la predicción del uso de ancho de banda.

# 5 Conclusiones finales

**Referencias**

[1] E. Coronado *et al.*, “Zero Touch Management: A Survey of Network Automation Solutions for 5G and 6G Networks,” *IEEE Commun. Surv. Tutor.*, vol. 24, no. 4, pp. 2535–2578, 2022.
[2] S. Dahmen-Lhuissier, “Zero touch network & Service Management (ZSM).” [Online]. Available: https://www.etsi.org/technologies/zero-touch-network-service-management.
[3] J. Kosińska, B. Baliś, M. Konieczny, M. Malawski, and S. Zieliński, “Toward the Observability of Cloud-Native Applications: The Overview of the State-of-the-Art,” *IEEE Access*, vol. 11, pp. 73036–73052, 2023.
[4] Z. Tao, W. Xu, Y. Huang, X. Wang, and X. You, “Wireless Network Digital Twin for 6G: Generative AI as a Key Enabler,” *IEEE Wirel. Commun.*, vol. 31, no. 4, pp. 24–31, Aug. 2024.
[5] M. Liyanage *et al.*, “A survey on Zero touch network and Service Management (ZSM) for 5G and beyond networks,” *J. Netw. Comput. Appl.*, vol. 203, p. 103362, July 2022.
[6] *Zero-touch network Service Management (ZSM); Enablers Artificial Intelligence-based Network Service Automation*. .
[7] P. Almasan *et al.*, “Network Digital Twin: Context, Enabling Technologies, and Opportunities,” *IEEE Commun. Mag.*, vol. 60, no. 11, pp. 22–27, Nov. 2022.
[8] C. Zhou *et al.*, “Network Digital Twin: Concepts and reference architecture,” *IETF Datatracker*. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-nmrg-network-digital-twin-arch/. [Accessed: 28-Sept-2025].
[9] “New ITU-T Recommendations for Digital Twin.” [Online]. Available: https://standict.eu/discussion-groups/digital-twin/321/new-itu-t-recommendations-digital-twin . [Accessed: 28-Sept-2025].
[10] Y. Goto, “Standardization activities on future networks in ITU-T SG13.” [Online]. Available: https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr202101gls.html. [Accessed: 28-Sept-2025].
[11] Y. Zhu, D. Chen, C. Zhou, L. Lu, and X. Duan, *A knowledge graph based construction method for Digital Twin Network*. 2021.
[12] R. Vilalta *et al.*, “Applying Digital Twins to Optical Networks with Cloud-Native SDN Controllers,” *IEEE Commun. Mag.*, vol. 61, no. 12, pp. 128–134, Dec. 2023.
[13] S. M. Raza, R. Minerva, N. Crespi, M. Alvi, M. Herath, and H. Dutta, “A comprehensive survey of Network Digital Twin architecture, capabilities, challenges, and requirements for Edge–Cloud Continuum,” *Comput. Commun.*, vol. 236, p. 108144, Apr. 2025.
[14] A. Cabellos and C. Janz, “Performance-oriented digital twins for packet and optical networks.” [Online]. Available: https://www.ietf.org/archive/id/draft-paillisse-nmrg-performance-digital-twin-02.html. [Accessed: 28-Sept-2025].
[15] H. Chai, H. Wang, T. Li, and Z. Wang, “Generative AI-Driven Digital Twin for Mobile Networks,” *IEEE Netw.*, vol. 38, no. 5, pp. 84–92, Sept. 2024.
[16] W. Wu, X. Huang, and T. H. Luan, “AI-native network digital twin for intelligent network management in 6G,” *arXiv [cs.NI]*, 02-Oct-2024.
[17] *Zero-touch network Service Management (ZSM); Network Digital Twin enhanced zero-touch network service management*. .
[18] *Zero-touch network Service Management (ZSM); Intent-driven autonomous networks*. .
[19] *Zero-touch network Service Management (ZSM); Closed-Loop Automation; Part 3: Advanced topics*. .
[20] *Zero-touch network Service Management (ZSM); Cross-domain E2E service lifecycle management*. .
[21] N. Saha, M. Zangooei, M. Golkarifard, and R. Boutaba, “Deep Reinforcement Learning

Approaches to Network Slice Scaling and Placement: A Survey," *IEEE Commun. Mag.*, vol. 61, no. 2, pp. 82–87, Feb. 2023.
[22] M. M. Roselló and M. Lorenzo, *Smart De-jittering using Network Digital Twin*. 2024.
[23] "About open digital architecture (ODA)." [Online]. Available: https://www.tmforum.org/oda/. [Accessed: 28-Sept-2025].
[24] "Open Networking Foundation," *Open Networking Foundation*, 19-June-2017. [Online]. Available: https://opennetworking.org/. [Accessed: 28-Sept-2025].
[25] "GSMA Networks." [Online]. Available: https://www.gsma.com/futurenetworks/. [Accessed: 28-Sept-2025].
[26] "OASIS topology and orchestration specification for cloud applications (TOSCA) TC." [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca. [Accessed: 28-Sept-2025].
[27] CasandraSoft Tech Solutions, "Automatización vs Personalización: Descubre el equilibrio perfecto." [Online]. Available: https://www.casandrasoft.com/blog-es/automatizacion-vs-personalizacion-como-encontrar-el-equilibrio-perfecto. [Accessed: 28-Sept-2025].
[28] B. Māris, "API - RouterOS - MikroTik documentation." [Online]. Available: https://help.mikrotik.com/docs/spaces/ROS/pages/47579160/API. [Accessed: 28-Sept-2025].
[29] *Automated Support Ticket System with Gmail, Trello, and Slack Notifications - N8N*. .
[30] "Error handling." [Online]. Available: https://docs.n8n.io/flow-logic/error-handling/. [Accessed: 28-Sept-2025].
[31] *N8N Pricing 2025: Complete Plans Comparison + Hidden Costs Analysis vs Alternatives*. .
[32] S. en Español, "14 estrategias de retención de clientes para aumentar tus beneficios," *Shopify*. [Online]. Available: https://www.shopify.com/es/blog/estrategias-retencion-clientes. [Accessed: 28-Sept-2025].
[33] "Automatiza procesos con n8n." [Online]. Available: https://www.abproject.com.ar/blog/automatiza-tus-procesos-con-n8n-guia-practica-para-pymes. [Accessed: 28-Sept-2025].