La IA agéntica transforma las operaciones de red de telecomunicaciones

WHITEPAPER
Traducción al español
Documento técnico

ust.com

UST

Resumen

Las redes de telecomunicaciones están escalando más rápido de lo que las operaciones tradicionales pueden gestionar. Los aumentos de tráfico, la diversificación de servicios y las expectativas crecientes de confiabilidad contrastan con una realidad: la mayoría de los operadores todavía dependen de flujos de trabajo manuales y basados en tickets que ralentizan la respuesta e incrementan los costos. El resultado es un modelo operativo optimizado para la visibilidad, no para una acción segura y oportuna.

Este documento presenta un modelo implementable para la IA agéntica: agentes de software que observan, razonan y actúan con seguridad en entornos de múltiples proveedores. A diferencia de los dashboards o de la automatización estática, la IA agéntica ofrece operaciones de bucle cerrado, controladas por objetivos de nivel de servicio (SLO), en las que cada acción es explicable, reversible y sujeta a políticas.

La arquitectura integra estándares de la industria, combinando analítica NWDAF de 3GPP, patrones de bucle cerrado ETSI ZSM/ENI y control O-RAN RIC. La gobernanza y la seguridad son elementos centrales: niveles de riesgo, controles de protección, aprobaciones por etapas, reversión automática ante regresiones de SLO y observabilidad continua mediante AgentOps.

Una hoja de ruta de adopción de 0 a 360 días comienza en un “modo sombra” de solo lectura, avanza a través de etapas de propuesta y aprobación, y culmina en una autonomía de bajo riesgo. Las métricas clave incluyen el MTTR (tiempo medio de resolución), la conversión de alertas en tickets, el consumo del presupuesto de errores, la eficiencia energética y el cumplimiento normativo.

Los resultados iniciales son prometedores. Los programas reportan reducciones de un orden de magnitud en el ruido de alertas, recuperación entre 15% y 30% más rápida, ahorros energéticos de dos dígitos en RAN y prevención predictiva de incidentes críticos. La IA agéntica permite a los operadores pasar de la supervisión centrada en dashboards a la ejecución orientada por intención, fortaleciendo la resiliencia, reduciendo el OPEX y sentando las bases para redes autónomas.

Tabla de contenidos

Resumen ejecutivo

Los operadores Tier-1 de Estados Unidos están mostrando que los cores nativos de la nube, las RAN virtualizadas y los despliegues de Open RAN escalan con rapidez. AT&T aspira a que alrededor del 70% del tráfico sea compatible con open-capable para 2026. Verizon gestiona decenas de miles de sitios vRAN con optimización energética asistida por IA, y T-Mobile impulsa la innovación RAN basada en IA junto con la expansión del acceso inalámbrico fijo.

A pesar de este progreso, los desafíos operativos persisten. Las interrupciones, los retrasos acumulados en tickets y las ineficiencias energéticas tensionan a los equipos y subrayan una verdad conocida: las redes reportan datos, pero los operadores no siempre pueden actuar sobre ellos de forma segura o eficiente. Los dashboards y los flujos de trabajo manuales quedan rezagados frente a despliegues dinámicos, lanzamientos frecuentes de funcionalidades y equipos heterogéneos de múltiples proveedores.

La IA agéntica inserta agentes inteligentes y sujetos a políticas dentro de los flujos de trabajo. Estos agentes observan la red, razonan dentro de objetivos de nivel de servicio definidos y actúan a través de interfaces aprobadas, con reversión automática si surgen riesgos de desempeño. Los resultados iniciales muestran reducciones drásticas en el ruido de alertas, resolución de incidentes más rápida, ahorros energéticos medibles y prevención predictiva de eventos críticos.

Al ir más allá de los dashboards hacia una ejecución orientada por intención, la IA agéntica transforma los centros de operaciones de red (NOC) de centros de monitoreo reactivo en motores proactivos, resilientes y rentables de confiabilidad de red.

Panorama del sector y puntos críticos de negocio

Las redes modernas de telecomunicaciones son cada vez más complejas. Los cores nativos de la nube, las RAN definidas por software y los equipos de proveedores diversos aumentan los posibles puntos de falla. Los runbooks exclusivamente humanos y la clasificación manual no pueden seguir el ritmo de los despliegues dinámicos, los lanzamientos frecuentes de funcionalidades ni la diversidad de proveedores.

Las capacidades de automatización están madurando:

- NWDAF (3GPP) cuantifica condiciones, pronostica riesgos e informa las operaciones del Core 5G
- ETSI ZSM proporciona patrones de automatización de bucle cerrado entre dominios
- El controlador inteligente O-RAN (RIC) separa la política no en tiempo real (A1) del control en tiempo casi real (E2), habilitando decisiones rápidas y localizadas

Combinados con la observabilidad moderna (logs, métricas, trazas y telemetría mediante OpenConfig/gNMI), los operadores pueden aplicar autonomía controlada. Los agentes proponen cambios con evidencia, ejecutan a través de interfaces aprobadas y revierten automáticamente si los SLO retroceden. El resultado: operaciones de bucle cerrado seguras, explicables y controladas por SLO.

La importancia es alta: cada incidente que escala a un puente nocturno afecta la experiencia del cliente, los costos operativos y la reputación de la marca. Las redes deben detectar problemas y actuar sobre ellos de forma segura y eficiente.

La restricción oculta: acción, no visibilidad

La mayoría de los NOC están saturados de datos: KPI, logs, trazas, traps de fallas y eventos de cambio fluyen hacia dashboards sofisticados. Sin embargo, ver el problema no es el cuello de botella: decidir qué hacer y ejecutarlo con seguridad sí lo es.

La toma de decisiones se fragmenta entre herramientas y dominios; la ejecución se ralentiza por runbooks frágiles, aprobaciones ad hoc y rollbacks ensayados de manera inconsistente. Los presupuestos de error rara vez condicionan la acción en tiempo real, por lo que la tolerancia al riesgo queda implícita. Previsiblemente, las tormentas de alertas se convierten en tormentas de tickets, el tiempo medio de reparación (MTTR) se extiende entre traspasos de equipos y las ventanas de cambio siguen siendo tensas.

La ejecución se vuelve aún más difícil por ecosistemas de proveedores fragmentados y procesos operativos aislados. Aunque la analítica NWDAF, la orquestación ZSM/ENI y las políticas RIC operan en distintas capas de red, convertir sus hallazgos en acciones automatizadas y unificadas suele exigir esfuerzo manual. Los operadores deben navegar múltiples interfaces, resolver recomendaciones contradictorias y mantener el cumplimiento, todo bajo la presión constante de reducir el downtime y sostener la continuidad del servicio.

La seguridad y la confiabilidad rara vez están incorporadas en los flujos de trabajo. Incluso pequeñas configuraciones erróneas o acciones retrasadas pueden propagarse por la red y afectar la calidad de experiencia (QoE) y el cumplimiento. Los procedimientos de reversión automática, el control por SLO y las aprobaciones por etapas se aplican de forma inconsistente, lo que obliga a los equipos a equilibrar velocidad y riesgo con información incompleta.

En resumen, la restricción no es la falta de visibilidad: los operadores ven la red. La restricción es la incapacidad de actuar de manera decisiva, segura y consistente a escala. Las redes generan datos mucho más rápido de lo que las operaciones tradicionales pueden convertirlos en acciones significativas y confiables. Esta brecha sustenta interrupciones en cascada, resolución lenta de incidentes y utilización subóptima de recursos.

Por qué falla el camino actual

Los NOC modernos tienen una visibilidad sin precedentes, pero siguen siendo reactivos. Las reglas basadas en umbrales desencadenan alarmas en cascada durante cambios de topología o picos de tráfico, lo que genera alertas casi duplicadas que requieren correlación manual. Sin aplicación en tiempo real de SLO y presupuestos de error, cada aviso parece urgente. Las herramientas fragmentadas obligan a operar cambiando de consola; incluso mitigaciones simples esperan aprobaciones ad hoc. Los rollbacks pocas veces ensayados elevan el riesgo percibido y ralentizan los lanzamientos nativos de la nube.

Las políticas RAN estáticas subutilizan energía y capacidad: las configuraciones de potencia fuera de hora pico desperdician kWh, y las configuraciones para picos limitan la QoE. Las tareas de cumplimiento, como paquetes de evidencia, verificación de mínimo privilegio y reconstrucción de incidentes, siguen siendo en gran medida manuales, desviando a ingenieros senior del trabajo preventivo hacia el papeleo.

El costo del statu quo

Cuando los incidentes de red dependen de llamadas nocturnas de emergencia y aprobaciones improvisadas, el costo humano es inmediato e inconfundible. Los ingenieros senior sufren agotamiento, y el conocimiento tácito queda concentrado en unas pocas personas; como resultado, la contratación y la retención se ven afectadas, ya que el mejor talento busca un equilibrio más saludable entre la vida laboral y personal. En respuesta, las organizaciones adoptan una gestión defensiva del cambio: congelamientos amplios durante periodos pico, prácticas cautelosas de rollback que ralentizan la recuperación y feature flags inactivos.

El mensaje implícito para la organización es claro: no confiamos en nuestra propia capacidad de actuar de forma segura y rápida. Esta desconfianza se amplifica cuando los clientes, o las redes sociales, reportan degradaciones del servicio antes de que el NOC las haya correlacionado, erosionando la confianza tanto en las herramientas como en las operaciones.

El impacto de negocio es igualmente tangible. Las demoras en la toma de decisiones extienden el MTTR, aumentan el riesgo de SLA e inflan los costos de soporte de terceros a medida que las alertas duplicadas generan colas de tickets en cascada. Los runbooks manuales y excesivamente cautelosos retrasan la recuperación de capacidad y comprometen la QoE. Las políticas RAN estáticas dejan energía y capacidad sin aprovechar, mientras las tareas de cumplimiento apartan a los ingenieros del trabajo preventivo y de la innovación estratégica.

En última instancia, la incapacidad de actuar de forma segura ralentiza el despliegue de servicios, prolonga los plazos de integración y reduce la confianza del liderazgo en las iniciativas de modernización. Cada nueva capacidad añade tanta incertidumbre como valor, creando un ciclo en el que el riesgo operativo se acumula junto con los costos de oportunidad.

Bucles cerrados explicables y controlados por SLO

Los desafíos descritos - conocimiento fragmentado, ejecución lenta y arriesgada, e ineficiencias operativas - evidencian una necesidad crítica: un marco que convierta la visibilidad en acciones seguras, medibles y automatizadas. El siguiente enfoque demuestra cómo la IA agéntica aborda estas restricciones sin comprometer la seguridad ni la gobernanza.

- **Sentir:** La red emite de forma continua telemetría alineada en el tiempo: mediciones de desempeño 3GPP, KPI de extremo a extremo, logs/métricas mediante OpenTelemetry, estado de dispositivos mediante OpenConfig/ gNMI y datos RIC KPM. Esta información se normaliza en un modelo estándar de servicio y topología, lo que habilita la correlación de eventos entre RAN, transporte y core

- **Comprender:** La detección de anomalías no supervisada, la correlación de cambios y el análisis causal/topológico identifican problemas. NWDAF cuantifica el impacto a nivel de slice y de usuario, promoviendo solo anomalías que amenazan los SLO
- **Razonar:** La evidencia se convierte en un plan de acción. Las opciones se evalúan frente a los SLO y los presupuestos de error; se calcula el impacto potencial (blast radius), se seleccionan despliegues canary y se predefinen las rutas de reversión
- **Actuar:** Las intenciones se ejecutan mediante el RIC Non-RT para orientación a nivel de política y el RIC near-RT para control rápido. SMO, OSS e ITSM ejecutan procedimientos estándar, con mecanismos de reversión automática si los SLO se degradan
- **Explicar:** Cada acción se anota con procedencia completa - estándares, MOP, tickets y resultados de pruebas - para garantizar auditabilidad y generar señales de aprendizaje que mejoren ciclos futuros

La seguridad y la resiliencia se diseñan dentro del sistema, no se presuponen. Los controles de protección segmentados por riesgo se alinean con marcos regulatorios y procesos formales de gobernanza, e incluyen:

- Evaluación de riesgos, controles de seguridad y revisiones éticas/de cumplimiento
- Restricciones en tiempo real mediante protecciones contra inyección de prompts, filtros de PII/sesgo y validadores de parámetros
- Intervención humana en el circuito para acciones de riesgo medio y alto

Los controles de protección impulsados por IA, cuando se implementan adecuadamente, han demostrado mejorar las velocidades de detección y recuperación hasta en un 90%, reduciendo el riesgo de acciones inseguras e interrupciones operativas. Los agentes se tratan como software de producción, supervisado mediante observabilidad AgentOps, que proporciona trazas, métricas, logs, detección de drift, contabilidad de recursos y mecanismos de chargeback unificados. En despliegues maduros, este enfoque ha demostrado una reducción de hasta el 90% en costos de downtime, ya que los incidentes se detectan antes, las remediaciones son reversibles por diseño y las acciones inseguras se bloquean antes de llegar a la red.

Arquitectura y modelo operativo de UST

UST traduce los conceptos de este documento en un modelo práctico e implementable para producción. La arquitectura está alineada con estándares, es neutral frente a proveedores y está diseñada para escalar con seguridad, permitiendo una adopción modular sobre inversiones existentes en OSS/NMS, SMO/RIC e ITSM sin una migración disruptiva:

- **SLO primero:** Cada decisión y cada cambio están condicionados por SLO explícitos y presupuestos de error
- **Explicable por defecto:** Todas las propuestas y acciones incluyen procedencia completa y trazas de auditoría
- **Reversible por diseño:** los despliegues canary, los límites de impacto (blast radius) y la reversión automática garantizan una ejecución segura.
- **Interfaces estándar:** NWDAF, patrones ETSI ZSM/ENI, O-RAN (A1/E2), OpenTelemetry, OpenConfig/gNMI
- **Niveles de intervención humana:** La autonomía escala de acuerdo con el riesgo y la evidencia

UAR SmartOps (AIOps agéntico para telecomunicaciones) y AgentOps Fabric

La base de UST orientada primero a la ejecución conecta los hallazgos directamente con acciones seguras y reversibles:

- **Capacidades de UST SmartOps:** detección de anomalías, correlación de tormentas de eventos, análisis de causa raíz (RCA) con evidencia documentada, predicción de fallos y ejecución de SOP/runbooks
- **Seguridad de la acción:** las intervenciones están condicionadas por SLO, se despliegan mediante canary y se revierten automáticamente si los SLO se degradan; los validadores de parámetros y políticas bloquean cambios inseguros
- **Columna vertebral de observabilidad:** un plano de datos unificado normaliza logs, métricas, trazas y telemetría en RAN, transporte y core
- **Controles AgentOps:** trazabilidad unificada de decisiones, ejecuciones sombra de preproducción, detección de drift, contabilidad de recursos y chargeback para una autonomía medible

Gobernanza de IA responsable para operaciones

La gobernanza está integrada para escalar la autonomía con seguridad:

- **Ruta formal de decisión:** evaluación de riesgos, protocolos de seguridad, revisión ética, comprobaciones de cumplimiento e informes de transparencia para cada agente y caso de uso
- **Controles de ejecución:** protecciones contra inyección de prompts, filtros de PII/sesgo, validadores de salida y parámetros, y límites de política por dominio

- **Niveles con intervención humana:** las rutinas de bajo riesgo se ejecutan automáticamente; el riesgo medio requiere aprobación; el riesgo alto exige doble control y rollback ajustado
- **Auditabilidad:** todas las recomendaciones y acciones referencian estándares, MOP y tickets, creando evidencia durable para reguladores y auditoría interna

Aceleradores de datos e integración

Los aceleradores simplifican la integración y mejoran la calidad de las decisiones cerrando brechas de contexto:

- **UST MPulse:** ingesta y enriquecimiento de ventanilla única, incluidos datos no estructurados, para habilitar correlación segura de incidentes, aprobaciones y actuación
- **R&S®SSV:** paquetes de evidencia y flujos de reporte automatizados para FCC/CPUC que reducen el trabajo operativo de cumplimiento
- **Touchstone:** benchmarking sintético CASS/core que correlaciona sondas con carga en vivo y eventos de cambio para anticipar incidentes y proponer mitigaciones

Control RAN/edge, optimización energética y modelo operativo 6.6

UST operacionaliza el control seguro en el edge y operaciones alineadas con resultados:

- Control alineado con RIC: rApps/xApps ajustan dinámicamente PRB, potencia, haces y ventanas de deep-sleep; las políticas Non-RT supervisan acciones near-RT; la QoE se protege mediante reversión automática controlada por SLO
- Orquestación entre dominios: los conectores SMO/OSS/ITSM ejecutan runbooks a través del transporte y el núcleo, utilizando despliegues canary y límites de impacto (blast radius)
- Plataforma de automatización centralizada: los SLO de plataforma, catálogos de cambios y créditos de servicio alinean incentivos; la entrega puede gestionarse de forma centralizada o federada con el NOC del cliente
- Impacto probado: los programas de referencia muestran reducciones significativas de MTTR, ahorros energéticos y alta disponibilidad de plataforma, traduciendo la arquitectura en ganancias medibles de OPEX y resiliencia

Gobernanza, seguridad y observabilidad

La autonomía efectiva requiere más que agentes inteligentes: exige un marco que gestione el riesgo, haga transparentes las acciones y haga responsable cada intervención. En entornos maduros de telecomunicaciones, la gobernanza está integrada en cada capa operativa, lo que permite que la IA agéntica escale con seguridad sin introducir riesgos imprevistos.

La segmentación por riesgo y las rutas de aprobación determinan cómo se aplica la autonomía. Las rutinas de bajo riesgo pueden ejecutarse automáticamente, las acciones de riesgo medio requieren aprobaciones por etapas con evidencia completa y las intervenciones de alto riesgo siguen medidas de doble control con ventanas de rollback más estrictas. Codificar estos umbrales permite a los operadores ampliar la autonomía sin comprometer la estabilidad de la red ni la QoE.

La seguridad se incorpora directamente en los agentes. Los controles de ejecución - protecciones contra inyección de prompts, filtros de PII y sesgo, y validadores de salida y parámetros - mantienen las intervenciones dentro de los límites de política. Los mecanismos de reversión automática deshacen acciones que amenazan los SLO, protegiendo el desempeño y la experiencia del usuario.

La observabilidad garantiza responsabilidad. Cada decisión de agente, desde la ingesta de telemetría hasta la actuación y el rollback, se traza y registra, creando una pista de procedencia completa para revisión interna y cumplimiento regulatorio. Las métricas monitorean seguridad, calidad, confiabilidad y costo, mientras la detección de drift, la reproducción offline y las pruebas A/B impulsan la mejora continua. Los mecanismos de chargeback hacen visibles los costos y beneficios de la autonomía entre equipos, y un interruptor de apagado permite la desconexión inmediata si se incumplen los SLO. Las revisiones posteriores a incidentes reconstruyen decisiones para validar seguridad y eficacia.

En conjunto, estas prácticas transforman la IA agéntica de un concepto teórico en un sistema operativo confiable. Los operadores pasan de dashboards reactivos a una ejecución proactiva y controlada por SLO, caracterizada por transparencia, resultados medibles y confianza en condiciones de alto riesgo. Las redes se gestionan verdaderamente, con resiliencia, cumplimiento y eficiencia operativa incorporados.

Conclusión

La IA agéntica no es otro dashboard; es el sistema operativo para la acción en telecomunicaciones. Al anclar cada intervención a SLO explícitos, aplicar controles de protección y aprobaciones, y proporcionar auditabilidad completa, los operadores pueden pasar de la visibilidad reactiva a una ejecución segura, reversible y orientada por intención.

Razones clave para actuar ahora:

- Las redes ya están evolucionando: cores nativos de la nube, actualizaciones de RAN y adopción de Open RAN
- La demora aumenta el costo: MTTR prolongado, energía desperdiciada y ciclos de cambio lentos
- Las expectativas de gobernanza y regulación están aumentando
- La unificación temprana de telemetría y procedencia crea ventajas de automatización defendibles
- La competencia ya aprende con rapidez, convirtiendo la flexibilidad nativa de la nube en palanca operativa

UST permite a los operadores acelerar la adopción, reducir el riesgo operativo y lograr resultados tangibles. Los programas han demostrado reducciones significativas del ruido de alertas, mejoras del 15% al 30% en MTTR, ahorros energéticos medibles en RAN y menor carga de cumplimiento. Al implementar IA agéntica alineada con estándares, sujeta a políticas y completamente observable, los operadores van más allá de los dashboards hacia operaciones reales orientadas por intención.

Libera todo el potencial de tu red y transforma la forma en que operan tus equipos: explora cómo UST SmartOps for Telcos puede ayudar a tu organización a lograr operaciones de telecomunicaciones más seguras, rápidas y eficientes a escala.

Referencias/bibliografía

1. AI-RAN Alliance. (2024, February 26). Industry leaders in AI and wireless form the AI-RAN Alliance.
2. AI-RAN Alliance. (2025, February 27). AI-RAN Alliance celebrates its first anniversary at MWC 2025.
3. Analysis Mason. (2025, May) Open Network Index: 2025 Results.
4. AT&T. (2023, December). AT&T collaborates with Ericsson to accelerate Open RAN in the U.S.
5. Capgemini Research Institute. (n.d.). Industrialization of RAN energy saving for greener connectivity at scale.
6. Capgemini Research Institute. (2024). Networks with intelligence [Report].
7. DevOps Research and Assessment (DORA). (2022). Accelerate: State of DevOps report 2022 [Report].
8. Ericsson. (n.d.). Ericsson Mobility Report (latest edition hub).
9. European Union. (2024). Artificial Intelligence Act (Regulation (EU) 2024/1689). EUR-Lex.
10. Federal Communications Commission. (2025, June 24). Disaster Information Reporting System (DIRS).
11. Google Cloud. (n.d.). Alerting on your error-budget burn rate.
12. Google SRE. (n.d.). Alerting on SLOs.
13. Google SRE. (n.d.). Error-budget policy for service reliability.
14. Google SRE. (n.d.). Implementing SLOs.
15. Legal Information Institute. (n.d.). 47 C.F.R. § 4.18 — Mandatory DIRS reporting. Cornell Law School.
16. Mobile World Live. (2025, February). AI-RAN Alliance momentum grows.
17. NEC. (2023). Reducing energy consumption in mobile networks. NEC Technical Journal.

18 National Institute of Standards and Technology (NIST). (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) [NIST AI 100-1].

19 National Institute of Standards and Technology (NIST). (n.d.). NIST AI RMF Playbook.

20 National Institute of Standards and Technology (NIST). (2024, July 26). AI Risk Management Framework: Generative AI profile (overview).

21 TM Forum. (2024). IG1443 — Autonomous Networks implementation guide (v7.0.0).

22 TM Forum. (n.d.). Autonomous Networks toolkit.

23 TM Forum. (2024). Autonomous Networks framework (IG1218F v2.0.0).

24 Verizon. (2022, September 12). Verizon deploys more than 8,000 vRAN cell sites; rapidly marches toward goal of 20,000+ by end-2025 [Press release].

Lista de abreviaturas

5G SA - 5G independiente (5G Standalone)

5GC - Core 5G

A/B - pruebas A/B (experimento controlado)

A1 - interfaz O-RAN de políticas/intenciones Non-Real-Time

AI - inteligencia artificial

AIOps - IA para operaciones de TI

AI-RAN - IA para redes de acceso radio (tema de alianza industrial)

AMF - función de gestión de acceso y movilidad en 5GC

AN - redes autónomas en el contexto de TM Forum

Auto-revert - rollback automático ante regresión de SLO; incluido para claridad

BLER - tasa de error de bloque

CASS - suite de benchmarking sintético de core; nombre en clave del programa en los materiales proporcionados

CPU - unidad central de procesamiento

CPUC - California Public Utilities Commission

E2 - interfaz O-RAN de control near-Real-Time

E2SM - modelo de servicio E2 (O-RAN)

EBITDA - ganancias antes de intereses, impuestos, depreciación y amortización

ENI - Experiential Networked Intelligence (ETSI)

EU - Unión Europea

FCC - Federal Communications Commission, EE. UU.

FWA - acceso inalámbrico fijo

gNB / gNodeB - estación base 5G

gNMI - gRPC Network Management Interface (OpenConfig)

GPU - unidad de procesamiento gráfico

ID - identificador

ITSM - gestión de servicios de TI

KMS - servicio de gestión de claves

KPI - indicador clave de desempeño

KPM - medición clave de desempeño (O-RAN, por ejemplo E2SM KPM)

kWh - kilovatio-hora

MOP - método de procedimiento

MTTD - tiempo medio de detección

MTTR - tiempo medio de reparación/restauración

NMS - sistema de gestión de red

NOC - centro de operaciones de red

Non-RT - no en tiempo real, dominio RIC

NWDAF - función de analítica de datos de red (3GPP)

Open RAN - arquitectura RAN desagregada/virtualizada

OPEX - gasto operativo

O-RAN - especificaciones de O-RAN Alliance para Open RAN

OSS - sistemas de soporte a operaciones

P95 - percentil 95

PDCP - Packet Data Convergence Protocol

PII - información de identificación personal

PRB - bloque de recurso físico

QoE - calidad de experiencia

R&S®SSV - automatización y reporte regulatorio; nombre en clave del programa en los materiales proporcionados

RAG - generación aumentada por recuperación

rApp - aplicación Non-RT RIC

RBAC - control de acceso basado en roles

RCA - análisis de causa raíz

RIC - controlador inteligente RAN

RLC - control de enlace de radio

RMF - marco de gestión de riesgos, por ejemplo NIST AI RMF

RRM - gestión de recursos radio

SLA - acuerdo de nivel de servicio

SLI - indicador de nivel de servicio

SLO - objetivo de nivel de servicio

SMO - gestión y orquestación de servicios (O-RAN/ORAN-SMO)

SON - red autoorganizada

SOP - procedimiento operativo estándar

SRE - ingeniería de confiabilidad de sitios

TM Forum (TMF) - organismo del sector para estándares y mejores prácticas de telecomunicaciones

TTL - tiempo de vida

VoNR - voz sobre New Radio, 5G

vRAN - RAN virtualizada

WORM - Write Once, Read Many

xApp - aplicación near-RT RIC

Juntos, construimos impacto sin límites

Desde 1999, en UST hemos trabajado junto a las mejores empresas del mundo para generar un impacto transformador. Impulsados por la tecnología, inspirados por las personas y guiados por nuestro propósito, colaboramos con nuestros clientes en cada etapa, desde el diseño hasta la operación. Nuestras soluciones digitales, plataformas propias, experiencia en ingeniería y ecosistema de innovación convierten los desafíos más complejos en soluciones disruptivas y de gran impacto. Con un profundo conocimiento de la industria y una mentalidad orientada al futuro, infundimos innovación y agilidad en las organizaciones de nuestros clientes, entregando valor tangible y generando un cambio positivo y duradero para ellos, sus clientes y las comunidades de todo el mundo. Juntos, con más de 30,000 empleados en más de 30 países, creamos un impacto ilimitado, transformando miles de millones de vidas en el proceso.

ust.com

Version 0102-20260612

U ▪
S T