



DOI: <https://doi.org/10.70577/cieninter.v4i3.133>

Diseño de una arquitectura nube-híbrida de alta disponibilidad para el monitoreo sísmico regional en el litoral ecuatoriano: análisis de red y hardware

Design of a high-availability hybrid-cloud architecture for regional monitoring in the ecuadorian coastal region: network and hardware analysis

Walter Vicente Mera Ortiz¹

Universidad Católica de Santiago de Guayaquil
walter.mera@cu.ucsg.edu.ec
<https://orcid.org/0000-0001-8063-4043>

Galo Enrique Cornejo Gómez²

Universidad Católica de Santiago de Guayaquil
galo.cornejo@cu.ucsg.edu.ec
<https://orcid.org/0000-0003-3523-2795>

José Miguel Erazo Ayón³

Universidad Católica de Santiago de Guayaquil
jose.erazo@cu.ucsg.edu.ec
<https://orcid.org/0000-0001-8288-9568>

Guillermo Alfonso Ponce Vásquez⁴

Universidad Católica de Santiago de Guayaquil
guillermo.ponce@cu.ucsg.edu.ec
<https://orcid.org/0000-0002-0936-5212>

Madelaine Alexandra Viera Gurumendi⁵

Universidad Católica de Santiago de Guayaquil
madelaine.viera@cu.ucsg.edu.ec
<https://orcid.org/0009-0002-1850-0639>

Cómo citar

Mera Ortiz, W. V., Cornejo Gómez, G. E., Erazo Ayón, J. M., Ponce Vásquez, G. A., & Viera Gurumendi, M. A. (2026). Diseño de una arquitectura nube-híbrida de alta disponibilidad para el monitoreo sísmico regional en el litoral ecuatoriano: análisis de red y hardware. *Ciencia Interdisciplinaria Internacional*, 4(3), 1217–1236. <https://doi.org/10.70577/cieninter.v4i3.133>

Fecha de recepción: 2026-08-24

Fecha de aceptación: 2026-09-07

Fecha de publicación: 2026-09-21

RESUMEN

El monitoreo sísmico en tiempo real es fundamental para reducir el riesgo de desastres y optimizar los sistemas de alerta temprana en zonas costeras con alta vulnerabilidad sísmica. Este artículo tuvo como objetivo diseñar, adaptar y validar en campo la infraestructura integral de hardware, telecomunicaciones y servidores en la nube del Centro de Monitoreo Sísmico (CEMSIS) para Guayaquil y sus estaciones remotas de Portoviejo y Manta. El estudio siguió un enfoque cuantitativo de ingeniería aplicada, organizado en cuatro fases: primero, la simulación del enrutamiento bajo una topología de estrella expandida en Cisco Packet Tracer; segundo, el acondicionamiento electrónico y calibración de los acelerógrafos REFTEK 130 y 130S con fuentes reguladas de 15 V DC / 3 A y conectores industriales Amphenol; tercero, el despliegue de conectividad redundante con conmutación por error mediante fibra óptica y 4G LTE a través de túneles OpenVPN cifrados con AES-256 hacia una instancia en la nube; y cuarto, la automatización del flujo continuo de datos con scripts de autorrecuperación bajo systemd. Los resultados demostraron que la arquitectura alcanzó una disponibilidad operativa del 99,9 % y transmitió señales continuas sin pérdida de paquetes, registrando latencias promedio de 25 a 30 ms en fibra y de 45 a 50 ms en los enlaces móviles, a un costo cercano a 9 USD mensuales por estación. Se concluye que el modelo híbrido elimina los puntos únicos de fallo y ofrece una solución escalable, cibersegura y económicamente sostenible para reforzar la resiliencia urbana ante eventos destructivos.

Palabras clave: Acelerógrafos, alta disponibilidad, computación en la nube, monitoreo sísmico, red privada virtual.

ABSTRACT

Real-time seismic monitoring is fundamental to reducing disaster risk and optimizing early warning systems along vulnerable coastal areas exposed to high seismic activity. This article aimed to design, adapt, and field-validate the comprehensive hardware, telecommunications and cloud-server infrastructure of the Seismic Monitoring Center (CEMSIS) for Guayaquil and its remote sensing stations in Portoviejo and Manta. The study followed a quantitative applied-engineering approach structured into four operational phases: first, routing simulation using an extended star topology within Cisco Packet Tracer; second, electronic conditioning, calibration, and stabilization of REFTEK 130 and 130S accelerographs using regulated 15 V DC / 3 A power supplies and industrial-grade Amphenol connectors; third, deployment of multi-carrier redundant connectivity featuring automated failover over fiber optics and 4G LTE cellular links via AES-256 encrypted OpenVPN tunnels toward a centralized cloud instance; and fourth, continuous stream automation through custom self-healing watchdog scripts operating under systemd. Empirical validation demonstrated that this architecture achieved 99.9% operational uptime and sustained continuous data transmission without packet loss, reporting average transmission latency of 25 to 30 ms across fiber backbones and 45 to 50 ms over mobile networks, at a maintenance cost of approximately 9 USD per station per month. Consequently, this hybrid edge-to-cloud model successfully removes single points of failure, delivering a highly scalable, robust, and cost-effective technological baseline to reinforce urban resilience and critical emergency decision-making during high-magnitude events.

Keywords: Accelerographs, cloud computing, high availability, seismic monitoring, virtual private network.

INTRODUCCIÓN

El litoral ecuatoriano constituye una de las zonas tectónicamente más activas del continente sudamericano. Guayaquil y su zona costera presentan una significativa vulnerabilidad ante sismos de gran magnitud debido a factores como su alta densidad demográfica, la concentración de infraestructura crítica y la complejidad geotécnica de sus suelos arcillosos estuarinos. Con este contexto, la medición precisa de la aceleración del suelo y la operatividad de los sistemas de alerta inmediata dependen de una red de sensores que transmitan datos de forma continua y segura. Esa red se apoya en acelerógrafos -es decir, sensores que miden la aceleración del suelo durante un sismo en tres ejes- y en un enlace de comunicaciones que lleva estos registros hasta un centro de procesamiento. La utilidad de una alerta temprana depende tanto de la calidad del sensor como del retardo total de la cadena de transmisión.

En concreto, el margen costero ecuatoriano se sitúa sobre la zona de subducción donde la placa de Nazca converge bajo la placa Sudamericana a una tasa cercana a 5 - 6 cm por año, lo que lo convierte en uno de los segmentos más activos del Pacífico sudamericano (Nocquet et al., 2017; Ye et al., 2016). El terremoto de Pedernales en abril de 2016, de magnitud 7,8 y con epicentro en Manabí dejó más de 600 víctimas y daños severos en Portoviejo y Manta. Esta situación evidenció los límites de los instrumentos disponibles en la región (Nocquet et al., 2017; Ye et al., 2016). Desde entonces, se ha señalado la necesidad de densificar la red de movimientos fuertes y asegurar que los datos lleguen sin interrupción a los centros de procesamiento, aun cuando se interrumpan las señales o la energía eléctrica local, condiciones frecuentes en la región.

En este contexto, a la exigencia de baja latencia se

suma la dificultad de instalar y mantener redes sísmicas en zonas costeras como Manabí. La mayor dificultad son los equipos antiguos que aún se utilizan, las conexiones obsoletas y la falta de repuestos originales. Por ejemplo, los acelerógrafos REFTEK, que requieren modificaciones eléctricas y cableado a medida para soportar las condiciones del clima en la costa. Asimismo, en sitios de difícil acceso que no cuentan con fibra óptica, resulta necesario desplegar enrutadores celulares 4G LTE enlazados mediante túneles de red privada virtual (VPN) cifrados, que previenen ataques y mantienen una sesión de conexión persistente con los servidores en la nube.

En el ámbito técnico actual, la ingeniería de instrumentación sismológica necesita superar los modelos tradicionales de almacenamiento local en servidores físicos universitarios, los cuales conllevan costos elevados de mantenimiento, escalabilidad limitada y una alta susceptibilidad ante cortes de energía eléctrica o caídas del servicio local de internet (Armbrust et al., 2010; Ni et al., 2025). Sin embargo, transmitir acelerogramas en tiempo real necesita de redes de telecomunicación estables y con baja latencia. En estos sistemas, cualquier fallo de la red pone en riesgo el monitoreo de los datos: depender de un único enlace introduce un punto único de fallo; además, sin mecanismos automáticos de recuperación, cada corte obliga a intervención manual y prolonga la interrupción del servicio.

Para comprender la magnitud de este reto, es fundamental revisar los antecedentes de la instrumentación geofísica. Tradicionalmente, los acelerógrafos (sensores de alta sensibilidad que miden la vibración del suelo) almacenaban la información en discos duros locales, lo que obligaba a los técnicos a viajar físicamente para extraer los datos tras un sismo (Havskov & Alguacil, 2016). En la última década, la

telemetría permitió enviar estos datos por internet; no obstante, su centralización en servidores físicos universitarios demostró ser vulnerable ante cortes eléctricos. Ante este escenario, la migración hacia la nube se plantea como alternativa, ya que la redundancia de servidores permite que el sistema siga operando aunque se pierda la energía local (Zhu et al., 2022).

En los últimos años varios grupos han migrado flujos de procesamiento sísmico hacia la nube pública. QuakeFlow demostró un flujo de detección y localización basado en aprendizaje automático ejecutándose de forma escalable sobre infraestructura de nube (Zhu et al., 2022); en la misma línea, se ha aplicado aprendizaje profundo al monitoreo sísmico en tiempo real durante secuencias de réplicas (Li et al., 2022). Ni et al. (2025) plantearon un enfoque “nativo de nube” para el manejo de grandes volúmenes de datos sismológicos, y Biondi et al. (2025) describieron el procesamiento en tiempo real de sensado acústico distribuido para operaciones de monitoreo. Estos trabajos se concentran en software de análisis; en casi ninguno de los casos mencionados se documenta cómo se construye y se sostiene la capa de transporte de datos en un territorio con energía y conectividad débiles. Wang et al. (2025), en este mismo contexto, exploraron modelos de lenguaje aplicados al monitoreo sísmico, y el abaratamiento de los sensores de movimiento fuerte, con instrumentos abiertos y de bajo costo (Bravo-Haro et al., 2021; Nesbitt et al., 2021), amplía el número de estaciones que una red regional debe sostener.

A diferencia de las propuestas centradas únicamente en algoritmos de procesamiento digital, este trabajo aborda la brecha técnica que surge al acoplar instrumentación física en el litoral con servicios en la nube: la alta salinidad costera, la inestabilidad

eléctrica y la obsolescencia de los conectores comprometen la adquisición de datos antes de que cualquier software pueda analizarlos. Frente a este escenario, se documenta la adaptación electromecánica, el enlace de red y la validación en campo de una arquitectura híbrida capaz de sostener telemetría continua. La infraestructura articula el reacondicionamiento eléctrico de los sensores en sitio, doble enlace fibra-celular por estación, un núcleo en AWS dividido entre transporte y procesamiento, junto con servicios bajo systemd programados para reordenar rutas y reconectar túneles de forma autónoma. Con ello, se plantea un esquema replicable y de bajo presupuesto para modernizar redes de movimiento fuerte sin depender de centros de cómputo locales ni renovación total del parque instrumental. Este planteamiento converge con los catálogos y estimaciones automáticas de magnitudes actuales (Bindi et al., 2024), así como con los marcos de monitoreo estructural interoperable (Blaso et al., 2021), aportando directamente a la resiliencia urbana ante amenazas geodinámicas (ODS 11).

El objeto de estudio de este trabajo es la infraestructura física y la red que sostiene a CEMSIS: los acelerógrafos y su alimentación, el cableado, los enrutadores de sitio, los enlaces redundantes y las instancias en la nube que reciben y almacenan datos. El alcance de esta primera fase se limita al diseño, la adaptación y la validación en campo del hardware y las telecomunicaciones en tres estaciones del litoral (Guayaquil, Portoviejo, Manta). Quedan fuera de esta fase el análisis sismológico de los registros y las herramientas de visualización para usuarios, que corresponden a una etapa posterior. La pregunta que guía este estudio es si una arquitectura nube-híbrida, con enlaces redundantes y recuperación automatizada, puede sostener una disponibilidad superior al 99% en

un entorno costero con energía y conectividad inestables.

Por consiguiente, la hipótesis del trabajo sostiene que una arquitectura en topología de estrella expandida, con conectividad redundante de fibra y 4G LTE, un núcleo virtual en la nube y rutinas automáticas de recuperación, elimina los puntos únicos de fallo y mantiene una disponibilidad operativa superior al 99 % en la red regional de estaciones, umbral tomado como referencia para infraestructura crítica alojada en la nube.

Para comprobarlo, el objetivo general de la investigación fue diseñar, adaptar y validar en campo una infraestructura híbrida de telecomunicaciones y hardware para el Centro de Monitoreo Sísmico (CEMSIS) que asegure la transmisión continua de datos en tiempo real desde Guayaquil, Portoviejo y Manta hacia un núcleo en la nube. Para alcanzar este propósito se establecieron cinco objetivos específicos: simular y validar el enrutamiento y el consumo de ancho de banda con una topología de red en estrella expandida; acondicionar física y eléctricamente los acelerógrafos de la serie REFTEK para soportar condiciones salinas en el entorno costero; desplegar túneles OpenVPN con enlaces redundantes de fibra óptica y 4G LTE hacia una instancia central en la nube; desarrollar automatizaciones (scripts) para la autorrecuperación de los servicios ante cortes de conexión o reinicios del servidor; y, por último, evaluar la arquitectura en términos de disponibilidad, latencia, pérdida de paquetes y costo operativo.

MATERIAL Y MÉTODOS

Esta investigación adoptó un enfoque cuantitativo bajo un diseño aplicado y tecnológico, orientado a resolver un problema concreto de ingeniería: dotar al CEMSIS de una infraestructura de transmisión de alta

disponibilidad y evaluar su desempeño a partir de indicadores numéricos verificables. La naturaleza cuantitativa del estudio se concretó transversalmente en sus cuatro fases metodológicas: la modelación de retardos sintéticos en la simulación; la verificación paramétrica de voltaje y corriente (15 V DC / 3 A) en laboratorio; la captura sistemática de latencia y pérdida de paquetes mediante sondas ICMP en la red; y el cómputo del porcentaje de disponibilidad operativa (*uptime*) y tiempos de conmutación en campo. El análisis se basó en la recolección y contraste de estas métricas frente a los umbrales fijados en el diseño. El estudio se orientó a la evaluación de la infraestructura y no incluyó sujetos de investigación: las pruebas recayeron directamente sobre los equipos, registrando suministro eléctrico, conectividad, retardos y estabilidad operativa en cada sede.

El sistema se desplegó en tres ciudades del litoral. Guayaquil albergó la estación central y una estación universitaria (UCSG); es la mayor área urbana del país y tiene suelos estuarinos blandos que amplifican el movimiento sísmico. Portoviejo y Manta, en Manabí, son estaciones remotas situadas cerca del segmento de ruptura del sismo de 2016 y dependen de una infraestructura de telecomunicaciones más limitada. Las tres estaciones se conectaron a un núcleo virtual alojado en la región us-east-1 de AWS. La distancia entre las sedes de Manabí y Guayaquil obligó a usar enlaces celulares como respaldo, ya que no todas cuentan con fibra óptica.

Los equipos se agrupan en cuatro conjuntos: instrumentación sísmica, red del sitio, enlaces de transporte y núcleo en la nube. Parte del hardware es heredado de la universidad y requirió adaptación; el resto se adquirió para esta fase. En la Tabla 1 se detallan las especificaciones técnicas iniciales y el rol operativo asignado a cada componente durante las

fases experimentales.

Tabla 1

Especificaciones técnicas de los equipos e instrumentación empleados en el banco de pruebas de CEMSIS

Conjunto	Equipo o material	Especificación principal	Función
Instrumentación	Acelerógrafo REFTEK 130 / 130S	Registrador de movimiento fuerte, tres ejes; alimentación +12 a +24 V DC	Adquisición de la aceleración del suelo
Instrumentación	Fuente regulada + conector Amphenol PT06A12-4P	Salida ajustada a 15 V DC / 3 A; cuatro pines roscados	Alimentación estable del acelerógrafo
Red de sitio	Módem NB2000 (heredado)	Firmware actualizado a la versión 1.2.3; enrutamiento avanzado	Interfaz de red local del acelerógrafo
Red de sitio	Cableado UTP Categoría 6	Norma T568B; conectores RJ45	Enlace físico a 1 Gbps en el sitio
Enlace primario	Enrutador TP-Link Omada	Políticas de calidad de servicio (QoS) sobre fibra óptica	Enlace principal de transporte
Enlace de respaldo	Enrutador Cudy 4G LTE	APN de operadora móvil; cifrado AES-256	Conmutación automática (failover) por red celular
Núcleo en la nube	AWS EC2 t2.micro	Amazon Linux 2023; 1 vCPU; 1 GiB RAM; IP pública estática; OpenVPN Access Server	Servidor de transporte / concentrador VPN
Núcleo en la nube	AWS EC2 t3.small	Windows Server 2022; 2 vCPU; 2 GB RAM; 60 GB SSD	Servidor de proceso y almacenamiento (software REFTEK)
Núcleo en la nube	AWS S3 + AWS Backup	Almacenamiento de objetos; respaldos programados	Respaldo redundante de los registros
Simulación	Cisco Packet Tracer	Modelado de topología y enrutamiento estático	Validación previa a la inversión

Nota. La familia t2/t3 corresponde a instancias de rendimiento con créditos de ráfaga de AWS. Elaboración propia.

Variables e indicadores. La evaluación se apoyó en cinco indicadores medibles, cada uno con un valor de referencia fijado en el diseño: la disponibilidad operativa, la latencia, la pérdida de datos, el consumo de recursos en la nube y el costo operativo por cada

estación. La Tabla 2 resume, para cada variable e indicador, el método de medición, el umbral de diseño y su justificación; estos valores sirvieron de referencia en la sección de Resultados.

Tabla 2

Variables, indicadores, umbrales de diseño y justificación

Variable o requisito	Indicador o especificación	Método de medición o referencia	Umbral / valor de diseño	Justificación
Disponibilidad operativa	Porcentaje de tiempo con transmisión activa (uptime)	Bitácoras del servicio de monitoreo (systemd)	≥ 99 %	Referencia para infraestructura crítica alojada en la nube
Latencia	Tiempo de ida y vuelta (RTT) al servidor EC2	Sondas ICMP cada 60 s desde cada enrutador	< 5 ms en el segmento local (objetivo de diseño); < 60 ms extremo a extremo (verificado)	Margen dentro del presupuesto de una alerta temprana

Pérdida de paquetes	Porcentaje de paquetes perdidos	Estadística de las sondas ICMP y del cliente REFTEK	0 % sostenido	Integridad de los acelerogramas
Consumo de recursos en la nube	Uso de CPU, memoria y red del servidor de proceso	Monitor de rendimiento de Windows Server	< 50 % de CPU	Capacidad para integrar nuevas estaciones
Costo operativo	USD mensuales por estación	Facturación de AWS + licencia de OpenVPN	≤ 10 USD por estación	Estructura de costo baja y predecible
Ancho de banda del enlace de sitio	Capacidad del enlace Ethernet	Certificación de enlace (norma IEEE 802.3)	1 Gbps	Transmisión en tiempo real de varios acelerógrafos sin encolamiento
Redundancia de enlace	Doble enlace por estación (fibra + 4G LTE)	Prueba de conmutación (failover)	Sin punto único de fallo	Eliminar el punto único de fallo del enlace
Seguridad de la transmisión	Túnel cifrado y autenticación	Configuración de OpenVPN	AES-256 con autenticación por certificado	Confidencialidad e integridad extremo a extremo
Escalabilidad	Integración de nuevas estaciones	Diseño de la arquitectura	Alta, sin reconfigurar el núcleo	Integrar estaciones sobre concentradores existentes

Nota. Los umbrales y valores se fijaron en la fase de diseño y sirvieron de referencia en la sección Resultados. Elaboración propia.

Para llevar un orden y asegurar que el proyecto pueda replicarse a futuro, el proyecto se dividió en cuatro etapas principales:

Fase 1: Diseño y simulación. Antes de empezar a modificar los equipos físicos, se modeló la topología en estrella expandida en Cisco Packet Tracer (Kamiloğlu, 2015). Se crearon nodos virtuales por cada estación. Además se configuraron tablas de enrutamiento estático hacia la subred de AWS (172.27.240.0/22), dentro del rango de direccionamiento privado (Internet Engineering Task Force, 1996).

Las pruebas consistieron en el envío sostenido de paquetes ICMP entre las sedes y el servidor central. El simulador reportó latencias internas cercanas a 0 ms, un valor que confirma la coherencia de las rutas; su

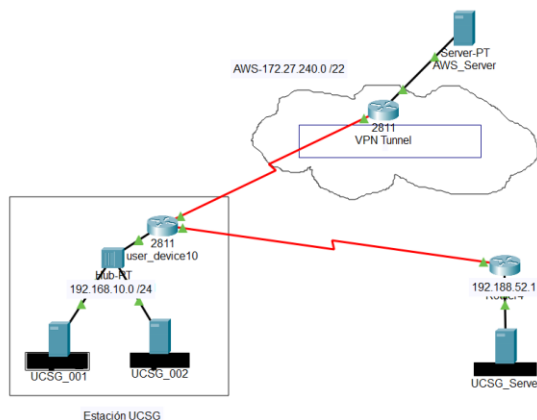
utilidad fue validar la viabilidad de la topología antes de comprometer la inversión en los equipos. Los requisitos técnicos que debía cumplir la red se recogen, junto con las variables e indicadores de evaluación, en la Tabla 2. El modelo de simulación se muestra en las Figuras 1 y 2.

En la simulación se estimó el consumo de ancho de banda por acelerógrafo, muy inferior a la capacidad del enlace de 1 Gbps previsto, lo que dio espacio para integrar nuevas estaciones sin rediseñar toda la red troncal.

El enlace de sitio se dimensionó sobre Ethernet a 1 Gbps conforme a la norma correspondiente (IEEE Standards Association, 2022), y el diseño de enrutamiento siguió prácticas establecidas de redes de datos (Kurose & Ross, 2017; Tanenbaum et al., 2021).

Figura 1

Diagrama de Topología de red estrella expandida



Nota. Elaboración propia a partir de la experiencia de operación del proyecto.

Figura 2

Modelo de simulación y pruebas de enrutamiento

Realtime Simulation										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	UCSG_001	AWS_Server	ICMP		0.000	N	0	(edit)	(delete)
	Successful	UCSG_002	AWS_Server	ICMP		0.000	N	1	(edit)	(delete)
	Successful	UCSG_001	UCSG_Server	ICMP		0.000	N	2	(edit)	(delete)

Nota. Elaboración propia a partir de la experiencia de operación del proyecto.

Fase 2: Adaptación en laboratorio. Como siguiente paso se procedió al acondicionamiento del hardware heredado, este constituyó un paso crítico para garantizar la compatibilidad con la nueva topología. Se preparó la red local de cada estación. El cableado se armó con par trenzado UTP Categoría 6 bajo la norma T568B, con conectores RJ45 de alta precisión. Las pruebas de conectividad y la certificación de enlace confirmaron una velocidad de 1 Gbps y bajo nivel de interferencia electromagnética. Los cables defectuosos detectados durante el crimpado se reemplazaron y se volvieron a probar. Los módems NB2000 heredados se inspeccionaron uno por uno. Además, se actualizó el firmware a la versión 1.2.3 y se ajustaron los parámetros de enrutamiento para habilitar rutas estáticas hacia la subred de AWS. De

tres unidades, dos quedaron sin observaciones y una presentó un daño estético en la carcasa que no afectó su funcionamiento.

El primer problema detectado en el hardware heredado era la alimentación de los acelerógrafos REFTEK 130 disponibles, estos carecían de los conectores originales y los componentes para realizar su acondicionamiento no se encontraban disponibles en el mercado nacional. La solución fue importar conectores industriales Amphenol PT06A12-4P de cuatro pines roscados y armar una fuente regulada a partir de los manuales del fabricante (REFTEK Systems, 2023). La Figura 3 reproduce la tabla de conectorización del manual. El conector admite un rango de +12 a +24 V DC, en este proyecto la salida se ajustó a 15 V DC y 3 A dentro del rango. La Tabla 3 detalla la asignación final de los

pinos. En Portoviejo y Manta se definió además una rutina de mantenimiento preventivo de los terminales metálicos, con blindaje mecánico y limpieza periódica

con solución anticorrosiva. El ajuste de la fuente regulada siguió criterios de calidad de la energía eléctrica (Dugan et al., 2012).

Tabla 3

Asignación de pines del conector Amphenol PT06A12-4P

Pin	Señal	Descripción
A	V+	Entrada positiva de voltaje (rango admitido +12 a +24 V DC; ajustada a 15 V DC)
B	V+	Entrada positiva (redundante con el pin A)
C	DGND	Retorno de tierra
D	DGND	Retorno de tierra (redundante con el pin C)

Nota. Elaboración propia a partir del manual del fabricante (REFTEK Systems, 2023). La fuente se ajustó a 15 V DC / 3 A.

Figura 3

Especificaciones de Conectorización del acelerógrafo.

1.5.1 Power connector

Power is supplied to the 1305 DAS unit through one power connector. Hardware connection shows typical hardware connection for the 1305 DAS. The following chart details individual connectors and REF TEK cable numbers.

Recorder Connector	Connector	1305 Pin	Pin Desc	Electrical Desc	Voltage Range
Power	PT06A12-4P	A	+12 VDC	Input	9-24 VDC
		B	+12 VDC	Input	9-24 VDC
		C	DGND	Power Return	
		D	DGND	Power Return	

Nota. Elaborado por REFTEK Systems (2023).

Fase 3: Configuración en la nube. Completada la adecuación electromecánica, se levantó el núcleo virtual en Amazon Web Services; este se dividió en dos instancias EC2 en la región us-east-1 (Ni et al., 2025). La primera, una t2.micro con Amazon Linux 2023, 1 vCPU y 1 GiB de memoria que funciona solo como servidor de transporte, ejecutaba OpenVPN Access Server sobre una IP pública estática y concentraba los túneles de las estaciones (Kotuliak et al., 2011). La segunda, una t3.small con Windows Server 2022, 2 vCPU, 2 GB de memoria y 60 GB de disco SSD, alojaba el software de gestión REFTEK y actuaba como servidor de proceso y almacenamiento

con respaldos hacia AWS Backup, su capacidad puede ampliarse según crezca la red. Separar el transporte del proceso evita que un pico de carga de análisis afecte la estabilidad de los túneles. El licenciamiento de OpenVPN se contrató en el plan Growth, que cubre diez licencias, una por enrutador de sitio, con un costo mensual de 9 USD por dispositivo licenciado. El servidor de proceso operaba bajo Windows Server 2022 para dar soporte al software de gestión sísmica (Silberschatz et al., 2018), mientras que el concentrador VPN se configuró con licencias dedicadas por enlace de sitio (Kotuliak et al., 2011; Mackey et al., 2020).

Tabla 4
Análisis comparativo de protocolos VPN para transmisión de datos en campo.

Criterio	OpenVPN	WireGuard	IPSec	PPTP
Compatibilidad	Amplia compatibilidad con routers, dispositivos móviles y sistemas operativos; soporte nativo en muchas soluciones de red.	Alta compatibilidad, pero menos soporte en routers más antiguos.	Compatibilidad moderada con routers, ampliamente usado en entornos corporativos.	Amplia compatibilidad, pero seguridad obsoleta.
Seguridad	Alto nivel de seguridad con cifrado AES-256, soporte para certificados y autenticación multifactor.	Seguridad robusta, pero menos maduro y auditado que OpenVPN.	Buena seguridad, pero más complejo de configurar correctamente.	Seguridad débil, vulnerable a ataques modernos.
Rendimiento	Buen rendimiento, optimizado para redes seguras y estables; puede ser configurado para optimización de velocidad.	Excelente rendimiento, especialmente en conexiones de alta latencia.	Rendimiento aceptable, pero puede ser pesado en recursos.	Rendimiento alto, pero a expensas de la seguridad.
Facilidad de Configuración	Configuración moderada; extensa documentación y soporte en la comunidad.	Fácil de configurar en algunos sistemas, pero carece de la extensa documentación de OpenVPN.	Complejo de configurar, especialmente en redes complejas.	Muy fácil de configurar, pero sin características avanzadas.
Soporte para Routers	Excelente, ampliamente soportado por la mayoría de los routers modernos y soluciones de red como pfSense y DD-WRT.	Limitado en comparación con OpenVPN, menos compatible con firmware de routers.	Soporte variable en routers, dependiendo de la implementación.	Soporte muy amplio, pero sin actualizaciones de seguridad.

Nota. Autoría Propia

Fase 4: Trabajo de campo. En la etapa final, el despliegue en las estaciones de Guayaquil, Manta y Portoviejo se ejecutó siguiendo los protocolos estandarizados de instalación geofísica (Instituto Geofísico, 2022). Se instalaron los enrutadores de conexión fija (TP-Link Omada) y los respaldos en móvil celular (Cudy 4G LTE). Además, se provocaron interrupciones controladas del servicio de internet para comprobar que el servidor lograra reconectarse automáticamente gracias a los scripts de recuperación programados. Los enrutadores celulares Cudy 4G LTE se configuraron como pasarelas de respaldo con mecanismos de conmutación transparente (failover), aplicando esquemas de enrutamiento resiliente en redes inalámbricas heterogéneas (Chanakitkarnchok et al., 2019; Qadir, 2015).

Durante el despliegue en campo se estandarizó el proceso de instalación de todas las

estaciones. Los pasos consistieron en: inspeccionar el sitio, verificar el hardware adquirido, montaje y aseguramiento de los equipos físicos, realizar el cableado, configurar la red e iniciar las pruebas de conexión mediante túneles cifrados. Tras finalizar cada paso se comprobaba que la estación pudiera enviar datos de forma ininterrumpida al sistema central.

El despliegue en Guayaquil, Portoviejo y Manta siguió un protocolo estandarizado de siete fases secuenciales: evaluación de condiciones ambientales y eléctricas del sitio; verificación de inventario según la Tabla 1; anclaje mecánico del instrumental y fijación de

conexiones a tierra; tendido de cableado estructurado; parametrización de red y credenciales locales; establecimiento del túnel OpenVPN; y validación del flujo de telemetría hacia la plataforma REFTEK en la nube. La transición entre etapas requirió la verificación previa del enlace para garantizar la continuidad operativa antes del cierre de visita.

Cada estación quedó configurada como un nodo que recolectaba los registros sísmicos y los enviaba a la nube por los dos enlaces redundantes descritos anteriormente, de esta forma que la caída de un enlace no interrumpía la transmisión.

La arquitectura de alta disponibilidad combinó la redundancia en las comunicaciones y la automatización lógica de los servicios en la nube a través de los siguientes componentes técnicos: En la estación principal se configuraron enrutadores empresariales TP-Link Omada con políticas de calidad de servicio (QoS) sobre enlaces de fibra óptica para priorizar la telemetría crítica frente a congestión de red

(Kurose & Ross, 2017). En las estaciones de Portoviejo y Manta se integraron routers industriales Cudy 4G LTE con cifrado AES-256 para la red móvil. Estos equipos operaron como enlace de respaldo (failover) y derivaron el tráfico automáticamente al detectar una caída de la conexión fija.

En relación al servidor alojado en AWS, se desarrolló un script en Bash configurado como un servicio de systemd. Su tarea principal era vigilar la estabilidad y la latencia del túnel VPN mediante pruebas ejecutadas cada 60 segundos. Además, el código se programó para soportar cortes de internet o reinicios del equipo siguiendo un orden estricto, cuando detectaba una caída, primero reconstruía las tablas de enrutamiento y volvía a levantar la conexión de OpenVPN. La recolección de los datos de los equipos REFTEK y los respaldos hacia AWS S3 no se iniciaban hasta que el sistema confirmaba la autenticación mediante certificados SSL. La estructura interna de este sistema de autorrecuperación se detalla en la Figura 4. El funcionamiento de esta rutina se resume en la Tabla 5.

Tabla 5

Pseudocódigo

cada 60 segundos:
enviar sonda al servidor VPN y medir latencia
si no hay respuesta o latencia supera el umbral:
1. reconstruir las tablas de enrutamiento hacia la subred de AWS 2. reiniciar el túnel OpenVPN 3. esperar confirmación de autenticación por certificado SSL 4. solo entonces: reanudar la recolección REFTEK y el respaldo a S3
registrar el evento en la bitácora

Nota. Elaboración propia a partir de la experiencia de operación del proyecto.



Figura 4

Lógica de recuperación para el restablecimiento de los servicios

```
#!/bin/bash
# Script de autoarranque y verificación de enlace CEMSIS (AWS EC2)
# Intervalo de monitoreo: 60 segundos

SERVER_IP="172.27.240.100"
LOG_FILE="/var/log/cemsis_recovery.log"

check_connection() {
    ping -c 3 $SERVER_IP > /dev/null 2>&1
    return $?
}

echo "[$(date)] Iniciando supervisión del enlace VPN CEMSIS..." >> $LOG_FILE

while true; do
    if ! check_connection; then
        echo "[$(date)] Alerta: Pérdida de conectividad detectada. Reiniciando túnel OpenVPN..." >> $LOG_FILE
        systemctl restart openvpn-client@aws_tunnel.service
        sleep 10

        if check_connection; then
            echo "[$(date)] Túnel OpenVPN autenticado (SSL verificado). Iniciando servicios REFTEK..." >> $LOG_FILE
            systemctl restart reftek-das.service
            systemctl restart aws-backup-sync.service
            echo "[$(date)] Secuencia de recuperación completada con éxito." >> $LOG_FILE
        else
            echo "[$(date)] Error crítico: No se pudo restablecer el túnel VPN. Reintentando en ciclo..." >> $LOG_FILE
        fi
    fi
    sleep 60
done
```

Nota. Elaboración propia a partir de la experiencia de operación del proyecto.

Protocolo de medición y análisis de datos

Además del procedimiento de instalación previamente comentado, la evaluación se apoyó en tres mediciones sistemáticas: la disponibilidad se calculó sobre el total de minutos de operación continua de la red, tomando como referencia las bitácoras del servicio de monitoreo generadas durante la Fase II del proyecto, y descontando los minutos sin transmisión; la latencia y pérdida de paquetes se obtuvieron de sondas ICMP ejecutadas cada 60 segundos desde cada enrutador hacia el servidor EC2, resumiéndose como promedio por estación; por su parte, la tolerancia a fallos se midió mediante pruebas controladas y repetidas de corte del enlace de fibra, cronometrando en cada una el tiempo que tardaba el sistema en conmutar a 4G y restablecer la transmisión. En cuanto a las consideraciones éticas, no participaron sujetos humanos ni se recopilaban datos personales: todas las pruebas se realizaron directamente sobre los equipos y la infraestructura tecnológica, por lo que el estudio no requirió aval de un comité de ética.

RESULTADOS

La evaluación técnica de la infraestructura CEMSIS arrojó resultados en los ejes definidos por los objetivos específicos: la simulación y el enrutamiento, la estabilidad electromecánica del hardware, el rendimiento de los enlaces redundantes, el consumo de recursos en la nube y la disponibilidad operativa. Todas las métricas obtenidas se compararon contra el estándar mínimo requerido para sistemas de alerta temprana.

Simulación y enrutamiento

El modelo en Cisco Packet Tracer reprodujo la topología con nodos virtuales por estación y rutas estáticas hacia la subred de AWS. El envío sostenido de paquetes ICMP arrojó latencias internas cercanas a 0 ms, un valor idealizado del simulador que confirmó la viabilidad de la topología y permitió proyectar un consumo de ancho de banda holgado frente al enlace de 1 Gbps antes de comprar los equipos.

Estabilidad electromecánica del hardware

El montaje de la topología en estrella expandida y la validación en campo de los acelerógrafos REFTEK 130S demostraron un rendimiento operativo altamente satisfactorio en las estaciones de Guayaquil, Portoviejo y Manta. La verificación eléctrica de las fuentes de alimentación con los conectores industriales Amphenol PT06A12-4P ratificó un suministro estable de 15 V DC / 3 A en todos los instrumentos, eliminando por completo las caídas de tensión y los reinicios espontáneos del hardware de

adquisición sísmica durante los muestreos continuos. Las inspecciones físicas periódicas confirmaron que el blindaje mecánico y los tratamientos anticorrosivos aplicados en los terminales evitaron el deterioro de los terminales por la salinidad en las estaciones costeras.

La verificación eléctrica y el estado de los conectores por estación se resumen en la Tabla 6; la fuente regulada entregó 15 V DC / 3 A en todos los instrumentos y los conectores con desgaste o daño se reemplazaron por completo.

Tabla 6

Verificación de alimentación y estado de los conectores por estación

Estación	Voltaje medido	Corriente medida	Estado del conector	Acción de mantenimiento	Resultado
Guayaquil – Sede Principal	15 V DC	3 A	Bueno	Limpieza e inspección	Operativo; sin caídas de tensión ni reinicios
Guayaquil – estación UCSG	15 V DC	3 A	Desgaste leve con corrosión incipiente	Reemplazo del conector Amphenol	Operativo tras el reemplazo
Portoviejo	15 V DC	3 A	Bueno	Limpieza e inspección	Operativo; transmisión estable
Manta	15 V DC	3 A	Dañado	Reemplazo del conector y prueba	Operativo tras el reemplazo

Nota. Elaboración propia a partir de la verificación eléctrica de laboratorio (Informe Mes 1) y del mantenimiento preventivo y correctivo de conectores en campo (Informe Mes 3). La fuente regulada entregó 15 V DC / 3 A en todos los instrumentos; los conectores con desgaste o daño se reemplazaron in situ.

Telecomunicaciones y enlaces redundantes

En el ámbito de las telecomunicaciones y la transmisión de información, el rendimiento del túnel OpenVPN cumplió con los parámetros de baja latencia requeridos por los protocolos de alerta temprana. Como se demuestra en la Tabla 7, la estación principal de Guayaquil registró latencias promedio entre 25 ms y 28 ms. En cambio, las estaciones remotas de Portoviejo y Manta reportaron tiempos de entre 45 ms y 50 ms. En todos los casos, los tiempos de respuesta

se mantuvieron muy por debajo del límite máximo permitido para procesar los datos sísmicos en tiempo real. Sobre el conjunto de siete enrutadores TP-Link Omada en enlaces de fibra, las latencias promedio hacia el servidor EC2 se ubicaron entre 25 ms y 30 ms, sin pérdida de datos una vez ajustadas las prioridades de QoS. Los tres enrutadores Cudy 4G LTE, sobre red celular, promediaron entre 45 ms y 50 ms; los valores más altos corresponden a los enlaces celulares y se estabilizaron ajustando la orientación de la antena. El

detalle por enrutador se presenta en la Tabla 7.

Tabla 7

Rendimiento de los enlaces redundantes por enrutador

Enrutador	Ubicación / estación	Enlace y direccionamiento	Protocolo / cifrado	Latencia media (ms)	Estado
TP-Link Omada 1	Guayaquil – Sede Principal	Fibra óptica / 192.168.1.0/24	OpenVPN / AES-256	25	Estable, sin pérdida de paquetes
TP-Link Omada 2	Guayaquil – estación UCSG	Fibra óptica / 192.168.2.0/24	OpenVPN / AES-256	28	Estable
TP-Link Omada 3	Guayaquil – nodo metropolitano 3	Fibra óptica / 192.168.3.0/24	OpenVPN / AES-256	30	Estable
TP-Link Omada 4	Guayaquil – nodo metropolitano 4	Fibra óptica / 192.168.4.0/24	OpenVPN / AES-256	28	Estable
TP-Link Omada 5	Guayaquil – nodo metropolitano 5	Fibra óptica / 192.168.5.0/24	OpenVPN / AES-256	30	Estable
TP-Link Omada 6	Guayaquil – nodo metropolitano 6	Fibra óptica / 192.168.6.0/24	OpenVPN / AES-256	25	Estable
TP-Link Omada 7	Guayaquil – nodo metropolitano 7	Fibra óptica / 192.168.7.0/24	OpenVPN / AES-256	25	Estable
Cudy 4G LTE 1	Portoviejo	4G LTE / APN de operadora móvil	OpenVPN / AES-256	45	Estable, reconexión automática
Cudy 4G LTE 2	Manta	4G LTE / APN de operadora móvil	OpenVPN / AES-256	50	Estable
Cudy 4G LTE 3	Portoviejo – enlace de respaldo	4G LTE / APN de operadora móvil	OpenVPN / AES-256	47	Estable

Nota. Elaboración propia a partir de los Informes Mes 3 y Mes 4. La latencia es el promedio de ida y vuelta hacia el servidor EC2 (región AWS us-east-1). Los siete enlaces de fibra corresponden al despliegue metropolitano de Guayaquil (192.168.1.0/24 a 192.168.7.0/24).

Cableado estructurado y red local de sitio

El cableado de cada nodo se ejecutó con par trenzado UTP Categoría 6 y conectores RJ45 de alta precisión bajo la norma T568B. Las pruebas de continuidad y la certificación de enlace confirmaron una velocidad de 1 Gbps con bajo nivel de interferencia electromagnética; los tramos de cable defectuosos detectados durante el crimpado se reemplazaron y se volvieron a probar. En paralelo, los tres módems NB2000 heredados se inspeccionaron uno por uno, se actualizó su firmware a la versión 1.2.3 y se ajustaron los parámetros de enrutamiento para habilitar rutas estáticas hacia la subred de AWS; dos unidades quedaron sin observaciones y una presentó un daño estético en la carcasa que no afectó su funcionamiento.

Con la red local lista, se ejecutaron pruebas de comunicación extremo a extremo desde un acelerógrafo hacia los tres destinos de la arquitectura: el enrutador Cudy 4G LTE, el servidor de la UCSG y el servidor central en AWS con Windows Server 2022. En los tres trayectos, las pruebas de ping y de transferencia resultaron exitosas, con comunicación estable y en tiempo real; los picos de latencia observados en los ensayos iniciales se corrigieron ajustando las prioridades de calidad de servicio y el ancho de banda. Estas pruebas confirmaron que la ruta de datos completa, instrumento, red de sitio, túnel cifrado y núcleo en la nube, quedaba operativa antes de iniciar la fase de campo.

Recursos en la nube y autorrecuperación

La evaluación de los servidores en la nube demostró un manejo eficiente de los recursos computacionales.

La instancia central EC2 t3.small, operando con

Windows Server 2022, mantuvo un uso de CPU promedio del 9 %. El uso de CPU se observa en la Figura 5

Figura 5

Monitor de rendimiento de la instancia EC2 t3.small en AWS.



Nota. Captura en tiempo real del uso de CPU, disco, red y memoria. Autoría propia

De la misma forma, el consumo de memoria física y las operaciones de red (E/S) se mantuvieron estables, lo que confirma que el sistema tiene capacidad para integrar nuevos sensores a la red.

El servicio de autorrecuperación se probó con cortes controlados y repetidos del enlace de fibra. En cada prueba el sistema reconstruyó las rutas, restableció el túnel OpenVPN, esperó la autenticación por

certificado y solo entonces reanudó la recolección REFTEK y el respaldo a S3, siempre en menos de un minuto y sin intervención manual. La Tabla 8 resume los servicios que arrancan de forma automática y su comportamiento ante un fallo. Los servicios se administraron con systemd conforme a las prácticas de gestión de servicios críticos en Linux (Love, 2013).

Tabla 8

Servicios configurados para autoarranque en el servidor central

Servicio	Función	Comportamiento ante un fallo
Software REFTEK	Recepción y procesamiento de datos sísmicos	Arranca automáticamente al iniciar el servidor
OpenVPN	Canal cifrado con las estaciones	Reconexión automática; se levanta antes que la recolección de datos
Respaldo (AWS Backup / S3)	Copia de los registros	Se ejecuta sin intervención; se reanuda tras restablecer el túnel
Monitoreo (watchdog systemd)	Vigila la latencia del túnel y el estado de los servicios	Registra el evento, reinicia el servicio caído y emite alerta

Nota. Elaboración propia. La rutina de vigilancia se ejecuta cada 60 segundos.

Disponibilidad operativa y respuesta ante incidentes

Sobre el total de minutos de operación continua de la red registrados en las bitácoras del servicio de monitoreo, y descontando los minutos sin transmisión,

la disponibilidad resultó del 99,9 %.

Para comprobar la respuesta de la arquitectura

ante incidencias operativas reales, se analizó un evento

de desconexión en la estación remota de Portoviejo. El sistema detectó cortes intermitentes en la recepción de datos sísmicos; al revisar los registros para descartar que se hubiera debido a una caída de la red celular 4G LTE, se determinó que el problema era un fallo de hardware en el módulo de comunicación interno del acelerógrafo local. Identificar esta incidencia a tiempo evitó que se perdiera la visibilidad de toda la red de la región, lo que permitió al centro de control activar un protocolo de reemplazo del equipo dañado sin afectar

Síntesis de resultados

En conjunto, la simulación confirmó la viabilidad de la topología y un consumo de ancho de banda holgado; el acondicionamiento eléctrico entregó 15 V DC / 3 A estables y eliminó los reinicios del hardware; los enlaces redundantes registraron latencias promedio de 25 a 30 ms en fibra y de 45 a 50 ms en 4G LTE, sin pérdida de paquetes; el servidor de proceso operó con un uso de CPU del 9 %; y la arquitectura alcanzó una disponibilidad operativa del 99,9 % con un costo cercano a 9 USD mensuales por estación, cumpliendo con los estándares exigidos para redes de alertas tempranas.

DISCUSIÓN

La principal contribución científica de este trabajo radica en demostrar la viabilidad técnica y económica de migrar las redes de monitoreo sísmico locales hacia entornos de computación en la nube pública, un modelo poco explorado en las infraestructuras de alerta temprana de la región.

Interpretación frente a la literatura

El hallazgo central de este estudio, una disponibilidad del 99,9% con latencias por debajo de 50 ms extremo a extremo, es consistente con Zhu et al. (2022); ese trabajo demuestra que un flujo de monitoreo sísmico

al funcionamiento del resto del sistema.

El caso es ilustrativo porque la causa no estaba en la red: las bitácoras del enrutador 4G no mostraban pérdidas de señal coincidentes con los cortes, lo que orientó el diagnóstico hacia el módulo de comunicación interno del acelerógrafo. La redundancia de enlaces y el monitoreo continuo de estado permitieron aislar y reemplazar el equipo sin perder visibilidad del resto de la red regional.

puede sostenerse de forma escalable sobre infraestructura de nube, y aquí se verifica en campo la capa de transporte que hace posible ese flujo. Biondi et al. (2025) señalan que la integración de datos en tiempo real para operaciones de monitoreo exige retardos cortos y enlaces estables; el presente trabajo cumple esa condición con la combinación de fibra y 4G LTE, en la que ningún enlace superó los 50 ms. La rutina de autorrecuperación reproduce el principio de los enfoques nativos de nube de Ni et al. (2025), sostener servicios científicos sin operación manual permanente, y en este caso se midió que restablece la transmisión en menos de un minuto tras un corte. Frente a los servidores universitarios tradicionales, que se detienen ante un corte eléctrico o una caída del proveedor, la arquitectura híbrida mantuvo la transmisión al no depender de un solo canal.

Seguridad de la transmisión

El túnel OpenVPN con cifrado AES-256 y autenticación por certificado protegió la integridad de los datos sin penalizar la latencia. Este resultado coincide con Mackey et al. (2020), quienes miden que OpenVPN conserva un rendimiento adecuado incluso en enlaces de alta latencia, como los enlaces móviles usados en Portoviejo y Manta. La conmutación de fibra a 4G se produjo sin pérdida de sesión, lo que confirma en la práctica lo que Stallings (2021) plantea

en el plano teórico: el cifrado extremo a extremo y la continuidad del servicio pueden coexistir en el mismo enlace.

Análisis económico

El costo de operación recurrente es del orden de 9 USD mensuales por estación y está dominado por la licencia de OpenVPN del plan contratado (una por enrutador); la instancia de transporte pertenece a la familia de bajo costo con créditos de ráfaga y el almacenamiento en

S3 es marginal frente a ese total. El desglose mensual detallado forma parte de los registros administrativos del proyecto. Frente a un servidor físico universitario, el modelo híbrido evita la inversión inicial en hardware, el costo de un sistema de respaldo eléctrico y el mantenimiento de una sala de datos, y traslada la redundancia a la nube. La Tabla 9 contrasta ambos modelos. Esa estructura de costo baja y predecible es la que hace viable escalar la red a más estaciones del litoral.

Tabla 9

Comparación: servidor físico universitario frente a arquitectura nube-híbrida

Criterio	Servidor físico universitario	Arquitectura nube-híbrida (CEMSIS)
Inversión inicial	Alta: servidor, respaldo eléctrico y sala acondicionada	Baja: sin compra de hardware propio
Respaldo eléctrico	UPS o planta propia de la institución	Incluido en la infraestructura del proveedor
Redundancia de datos	Manual y local	Copias múltiples en S3
Escalar la red	Requiere recompra de hardware	Añadir una instancia o rutas
Corte eléctrico regional	El sistema se detiene	Sigue operando
Costo mensual	Variable y poco predecible	~9 USD por estación, previsible
Punto único de fallo	Servidor y enlace únicos	Enlaces redundantes + autorrecuperación

Nota. Elaboración propia a partir de la experiencia de operación del proyecto.

Hallazgos de hardware en ambiente salino

La corrosión de los terminales metálicos apareció con rapidez en las estaciones costeras. La experiencia confirma que operar en el litoral ecuatoriano obliga a aplicar blindaje mecánico y limpiezas químicas periódicas para evitar cortocircuitos y pérdida de señal; sin ese mantenimiento preventivo, la ganancia de disponibilidad que aporta la redundancia de enlaces se pierde en el eslabón más simple de la cadena. El incidente de Portoviejo, causado por el módulo de comunicación interno de un acelerógrafo y no por la red, apunta en la misma dirección: el instrumento

sigue siendo un punto sensible.

Aporte metodológico

Más allá de las cifras, el trabajo deja un protocolo de despliegue replicable: un guion de siete pasos que se aplicó sin variación en las tres estaciones, en el que cada paso se verificaba antes de avanzar al siguiente. Esa disciplina de certificación por etapas permitió aislar con rapidez el incidente de Portoviejo y explica buena parte de la disponibilidad alcanzada. Para redes de movimiento fuerte que crecen estación por estación en territorios de acceso difícil, disponer de un

procedimiento estandarizado, documentado y verificable es tan valioso como la propia arquitectura de hardware.

Limitaciones y validez externa

La estabilidad de las estaciones que dependen de 4G LTE está atada a la cobertura de las operadoras comerciales en la costa. Aunque el sistema reconecta ante cortes breves, un sismo de gran magnitud podría saturar las redes celulares públicas y retrasar la llegada de datos justo cuando más se necesitan. El periodo de observación de esta fase es acotado; una evaluación de varios meses, con métricas de jitter y con más estaciones, permitiría confirmar que el 99,9 % se sostiene en el tiempo. Las latencias del simulador (cercanas a 0 ms) son idealizadas y no incluyen la distancia real hasta la región de nube. Los resultados son extrapolables a otras redes de movimiento fuerte en contextos con energía y conectividad débiles, pero los valores concretos de latencia dependen de la región de nube elegida y de la operadora móvil local.

CONCLUSIONES

Cada objetivo específico se cumplió. La simulación en Cisco Packet Tracer validó la topología en estrella expandida y permitió dimensionar el enrutamiento y el ancho de banda antes de invertir en equipos. El acondicionamiento de los acelerógrafos REFTEK con conectores Amphenol regulados a 15 V DC / 3 A resolvió el problema de alimentación con bajo presupuesto y eliminó los reinicios espontáneos. Los túneles OpenVPN con enlaces redundantes de fibra y 4G LTE sostuvieron la transmisión cifrada extremo a extremo con latencias por debajo de 50 ms y conmutación automática sin pérdida de sesión. Los scripts de autorrecuperación bajo systemd devolvieron el servicio a la normalidad en menos de un minuto tras cortes o reinicios, sin intervención humana. En

conjunto, la arquitectura alcanzó una disponibilidad operativa del 99,9 % con un costo de operación cercano a 9 USD mensuales por estación, lo que confirma la hipótesis de partida.

Perspectivas de estudio y trabajos futuros

Con la capa de hardware y telecomunicaciones ya validada, la investigación continúa en tres frentes. El primero es una evaluación de disponibilidad de largo plazo, de al menos seis meses, que incorpore métricas de jitter y variación de latencia y que amplíe la red a nuevas estaciones del litoral. El segundo es reforzar la autonomía energética de las estaciones remotas con respaldo solar o sistemas de alimentación ininterrumpida dimensionados para la costa. El tercero es la integración formal de la red con los organismos nacionales de vigilancia sísmica mediante acuerdos de nivel de servicio. Estos avances consolidan el aporte del proyecto a la reducción del riesgo de desastres y a la construcción de ciudades más seguras (ODS 11).

REFERENCIAS BIBLIOGRÁFICAS

- Armbrust, M., Stoica, I., Zaharia, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., & Stoica, I. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50–58. <https://doi.org/10.1145/1721654.1721672>
- Bindi, D., Zaccarelli, R., Strollo, A., Di Giacomo, D., Heinloo, A., Evans, P., Cotton, F., & Tilmann, F. (2024). Enriching the GEOFON seismic catalog with automatic energy magnitude estimations. *Earth System Science Data*, 16(4), 1733–1745. <https://doi.org/10.5194/essd-16-1733-2024>
- Biondi, E., Tepp, G., Yu, E., Saunders, J. K., Yartsev, V., Black, M., Watkins, M., Bhaskaran, A.,



- Bhadha, R., Zhan, Z., & Husker, A. L. (2025). *Real-time processing of distributed acoustic sensing data for earthquake monitoring operations*. arXiv. <https://doi.org/10.48550/arXiv.2505.24077>
- Blaso, L., Clemente, P., Giovinazzi, S., Giuliani, G., & Gozo, N. (2021). Towards standardized and interoperable platforms for supporting the seismic vulnerability assessment and seismic monitoring of Italian bridges and viaducts. En *Lecture Notes in Civil Engineering* (pp. 471–480). Springer. https://doi.org/10.1007/978-3-030-91877-4_54
- Bravo-Haro, M. A., Ding, X., & Elghazouli, A. Y. (2021). MEMS-based low-cost and open-source accelerograph for earthquake strong-motion. *Engineering Structures*, 230, 111675. <https://doi.org/10.1016/j.engstruct.2020.111675>
- Chanakitkarnchok, A., Kawila, K., Sato, G., Owada, Y., & Charnsripinyo, C. (2019). Disaster-resilient communication framework for heterogeneous vehicular networks. En 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC) (pp. 1–6). IEEE. <https://doi.org/10.1109/PIMRC.2019.8904211>
- Dugan, R. C., McGranaghan, M. F., Santoso, S., & Beaty, H. W. (2012). *Electrical power systems quality* (3.^a ed.). McGraw-Hill.
- Havskov, J., & Alguacil, G. (2016). *Instrumentation in earthquake seismology* (2.^a ed.). Springer. <https://doi.org/10.1007/978-3-319-21314-9>
- IEEE Standards Association. (2022). *IEEE Std 802.3: Ethernet standards*. IEEE.
- Instituto Geofísico de la Escuela Politécnica Nacional. (2022). *Manual de procedimientos para la instalación y mantenimiento de acelerógrafos en campo*. Escuela Politécnica Nacional. <https://www.igepn.edu.ec/acelerografos>
- Internet Engineering Task Force. (1996). *RFC 1918: Address allocation for private internets*. <https://www.rfc-editor.org/rfc/rfc1918>
- Kamiloğlu, M. E. (2015). Cisco network performance evaluation using Packet Tracer. *International Journal of Electronics, Mechanical and Mechatronics Engineering*, 5(1), 905–911. <https://doi.org/10.17932/IAU.IJEMME.m.21460604.2015.5/1.905-911>
- Kotuliak, I., Rybár, P., & Trúchly, P. (2011). Performance comparison of IPsec and TLS based VPN technologies. En 2011 9th International Conference on Emerging eLearning Technologies and Applications (ICETA) (pp. 217–221). IEEE. <https://doi.org/10.1109/ICETA.2011.6112567>
- Kurose, J. F., & Ross, K. W. (2017). *Computer networking: A top-down approach* (7.^a ed.). Pearson.
- Li, W., Koehler, J., Chakraborty, M., Quinteros-Cartaya, C., Rümpler, G., & Srivastava, N. (2022). *Real-time earthquake monitoring using deep learning: A case study on the Turkey earthquake aftershock sequence*. arXiv. <https://doi.org/10.48550/arXiv.2211.09539>
- Love, R. (2013). *Linux system programming: Talking directly to the kernel and C library* (2.^a ed.). O'Reilly Media.
- Mackey, S., Mihov, I., Nosenko, A., Vega, F., & Cheng, Y. (2020). A performance comparison of WireGuard and OpenVPN. En *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy* (pp. 162–164). Association for Computing Machinery.



- <https://doi.org/10.1145/3374664.3379532>
- Nesbitt, I., Boaz, R., & Long, J. (2021). rsudp: A Python package for real-time seismic monitoring with Raspberry Shake instruments. *Journal of Open Source Software*, 6(68), 2565. <https://doi.org/10.21105/joss.02565>
- Ni, Y., Denolle, M. A., Münchmeyer, J., Wang, Y., Feng, K.-F., Garcia Jurado Suarez, C., Thomas, A. M., Trabant, C., Hamilton, A., & Mencin, D. (2025). A review of cloud computing and storage in seismology. *Geophysical Journal International*, 243(1), ggaf322. <https://doi.org/10.1093/gji/ggaf322>
- Nocquet, J.-M., Jarrín, P., Vallée, M., Mothes, P. A., Grandin, R., Rolandone, F., Delouis, B., Yepes, H., Font, Y., Fuentes, D., Régnier, M., Laurendeau, A., Cisneros, D., Hernández, S., Sladen, A., Singaicho, J.-C., Mora, H., Gómez, J., Montes, L., & Charvis, P. (2017). Supercycle at the Ecuadorian subduction zone revealed after the 2016 Pedernales earthquake. *Nature Geoscience*, 10(2), 145–149. <https://doi.org/10.1038/ngeo2864>
- Qadir, J. (2015). Artificial intelligence based cognitive routing for cognitive radio networks. *Artificial Intelligence Review*, 45(1), 25–96. <https://doi.org/10.1007/s10462-015-9438-6>
- REFTEK Systems. (2023). *Manual de usuario de REFTEK 130S y 130S-DC: Configuración y manejo de datos sísmicos*. REFTEK Systems Inc. <https://manuals.reftek.com/category/130S/>
- Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). *Operating system concepts* (10.^a ed.). Wiley.
- Stallings, W. (2021). *Network security essentials: Applications and standards* (6.^a ed.). Pearson.
- Tanenbaum, A. S., Feamster, N., & Wetherall, D. J. (2021). *Computer networks* (6.^a ed.). Pearson.
- Wang, X., Liu, F., Su, R., Wang, Z., Fang, L., Zhou, L., Bai, L., & Ouyang, W. (2025). *SeisMoLLM: Advancing seismic monitoring via cross-modal transfer with a pre-trained large language model*. arXiv. <https://doi.org/10.48550/arXiv.2502.19960>
- Ye, L., Kanamori, H., Avouac, J.-P., Li, L., Cheung, K. F., & Lay, T. (2016). The 16 April 2016, Mw 7.8 Ecuador earthquake: A quasi-repeat of the 1942 Ms 7.5 earthquake and partial re-rupture of the 1906 Ms 8.6 Colombia–Ecuador earthquake. *Earth and Planetary Science Letters*, 454, 248–258. <https://doi.org/10.1016/j.epsl.2016.09.006>
- Zhu, W., Hou, A. B., Yang, R., Datta, A., Mousavi, S. M., Ellsworth, W. L., & Beroza, G. C. (2022). *QuakeFlow: A scalable machine-learning-based earthquake monitoring workflow with cloud computing*. arXiv. <https://doi.org/10.48550/arXiv.2208.14564>