https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 24 - 46

Implementación de un sistema automatizado de monitoreo de red multi-sede en una institución universitaria

Implementation of an automated multi-site network monitoring system in a university institution

Información del reporte:

Licencia Creative Commons

El contenido de los textos es responsabilidad de los autores y no refleja forzosamente el punto de vista de los dictaminadores, o de los miembros del Comité Editorial, o la postura del editor y la editorial de la publicación.

Para citar este reporte técnico:

López Ibarra, J. G. y Velázquez Portilla, D. (2026). Implementación de un sistema automatizado de monitoreo de red multi-sede en una institución universitaria. *Cuadernos Técnicos Universitarios de la DGTIC, 4*(3), páginas (24 - 46). https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181

Jorge Gerardo López Ibarra
Instituto de Biología
Universidad Nacional Autónoma de México
jlopez@ib.unam.mx
ORCID: 0009-0004-4703-4993

David Velázquez Portilla
Instituto de Biología
Universidad Nacional Autónoma de México
davepo@ib.unam.mx
ORCID: 0009-0009-8467-8225

Resumen

En una entidad universitaria con varias sedes y entornos de operación, el monitoreo de los servicios digitales dependía de una revisión técnica dispersa: consultas separadas en distintas plataformas, registros manuales y validaciones periódicas. Eso hacía difícil tener una visión clara del estado general de la red. Para resolver esta situación, se diseñó e implementó un sistema automatizado que integró fuentes de información heterogéneas, normalizó datos operativos y generó indicadores semanales para cinco entornos institucionales.

La metodología se organizó en las etapas de diseño, configuración, instalación y pruebas, con énfasis en la reutilización de herramientas existentes, la protección de información sensible y la elaboración de una visualización ejecutiva del entorno. Esta implementación permitió disminuir la dependencia de procesos manuales, consolidar información técnica dispersa y apoyar el seguimiento operativo de la red institucional.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 **Vol. 4, Núm. 3.** julio-septiembre 2026, págs. 25 - 46

Palabras clave: Automatización de operaciones, gestión de servicios tecnológicos, indicadores de disponibilidad, redes universitarias, visualización ejecutiva.

Abstract

In a university entity with several sites and operational environments, monitoring digital services relied on a fragmented technical review process involving separate queries across different platforms, manual records, and periodic validations. This made it difficult to obtain a clear view of the overall network status. To address this situation, an automated system was designed and implemented to integrate heterogeneous information sources, normalize operational data, and generate weekly indicators for five institutional environments. The methodology was organized into the stages of design, configuration, installation, and testing, with emphasis on reusing existing tools, protecting sensitive information, and producing an executive visualization of the environment. This implementation reduced dependence on manual processes, consolidated dispersed technical information, and supported operational monitoring of the institutional network.

Keywords: *Operations automation, technology service management, availability indicators, university networks, executive visualization.*

1. INTRODUCCIÓN

La correcta operación de los servicios digitales en las instituciones de educación superior depende, cada vez con mayor intensidad, de redes de datos estables, puntos de acceso inalámbrico disponibles y enlaces de comunicación capaces de atender actividades académicas, administrativas y de investigación. En este contexto, el monitoreo técnico dejó de ser una actividad aislada de revisión de equipos y se convirtió en un proceso necesario para garantizar el óptimo desempeño de los servicios institucionales. Como ha señalado la literatura reciente, contar con información integrada ayuda a tomar decisiones y responder mejor ante fallas en entornos complejos (Farahmand *et al*., 2022; Ta-Armart y Savithi, 2026).

El Instituto de Biología de la Universidad Nacional Autónoma de México (IBUNAM) opera sus servicios de red en espacios con condiciones distintas de conectividad, ubicación geográfica y administración tecnológica. A la infraestructura ubicada en Ciudad Universitaria, se sumaron estaciones foráneas y espacios especializados que utilizaron plataformas de gestión diferentes. Esta diversidad hizo que la supervisión dependiera de consultas en herramientas por separado de revisión de reportes de tráfico, inspección de consolas de administración inalámbrica y captura de información complementaria para sedes con condiciones particulares.

Aunque ya se cuentan con herramientas de administración y monitoreo, la información no se encontraba integrada en una sola vista. Esta situación dificultaba comparar el comportamiento entre sedes, construir históricos semanales y presentar indicadores comprensibles para seguimiento técnico y administrativo. En la práctica, el personal responsable debía dedicar tiempo a recopilar datos de distintas fuentes, validar su consistencia y preparar reportes de forma manual. Este esquema funcionaba, pero no era suficiente para responder con agilidad y rapidez a una infraestructura distribuida que cambiaba de manera constante.

Diversos trabajos recientes propusieron arquitecturas modulares, tableros de visualización y mecanismos automáticos de recolección de datos para mejorar la administración de servicios tecnológicos. Estas

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 26 - 46

propuestas coincidieron en separar la adquisición de datos, el procesamiento y la visualización para facilitar la escalabilidad y reducir errores operativos en redes institucionales y entornos de campus (Boluda-Prieto *et al*., 2026; Espinel-Villalobos *et al*., 2022; Lee *et al*., 2014; Rafiq *et al*., 2025; Witczak *et al*., 2024). En el caso universitario analizado, esa aproximación permitió plantear una solución ajustada a las herramientas disponibles, sin tener que sustituir por completo las plataformas existentes.

En el contexto del IBUNAM, estos desafíos no se expresaron como un problema abstracto de arquitectura tecnológica, sino como una necesidad operativa concreta: consultar entornos multi-marca, reunir datos de sedes con diferentes condiciones de conectividad y conservar evidencia periódica del estado de la red. Por ello, el proyecto se orientó a una analítica semanal estructurada, sin sustituir el diagnóstico operativo inmediato que permanece en las consolas especializadas de cada plataforma.

El objetivo del proyecto fue implementar un sistema automatizado de monitoreo de red multi-sede que integrara información proveniente de plataformas heterogéneas, generara indicadores semanales y presentara una visualización ejecutiva para fortalecer la supervisión operativa de servicios tecnológicos en una institución universitaria.

El proyecto se desarrolló durante el periodo 2025-2026 y se concentró en la construcción de un reporte semanal de estado de red para cinco entornos institucionales, ubicados en Ciudad de México, Jalisco, Colima y Veracruz. El alcance se limitó a indicadores operativos generales de conectividad, disponibilidad, infraestructura inalámbrica y comportamiento de enlaces, sin exponer configuraciones internas, direcciones sensibles, credenciales ni detalles que comprometieran la seguridad de la institución.

2. DESARROLLO TÉCNICO

Para dar mayor orden a la exposición, el desarrollo técnico se presenta en dos niveles. Primero, se explican los términos generales, la base conceptual y el modelo de procesamiento que puede aplicarse a un sistema automatizado de monitoreo multi-sede. Después, se muestra cómo esos principios se aplicaron al caso específico del IBUNAM mediante las etapas de diseño, configuración, instalación y pruebas.

Esta organización permite distinguir entre la teoría que sustenta la solución y la forma en que dicha teoría se convirtió en una herramienta operativa. De esta manera, el reporte no presenta únicamente un producto final, sino el razonamiento técnico que permitió pasar de plataformas separadas a una visualización semanal integrada.

2.1 TÉRMINOS GENERALES Y BASE CONCEPTUAL

Monitoreo de red

Seguimiento periódico de indicadores que permiten conocer el estado general de la conectividad, los dispositivos de red y los servicios asociados. No se limita a observar si un equipo está encendido o apagado; también considera tendencias, disponibilidad, clientes conectados, comportamiento de enlaces y observaciones que ayudan a interpretar la operación de una infraestructura tecnológica.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 27 - 46

Entorno multi-sede

Condición operativa en la que la información proviene de espacios con conectividad, proveedores, equipos, mecanismos de administración y niveles de automatización diferentes. Esta característica dificulta la comparación cuando la revisión se realiza de manera manual o aislada.

Fuente heterogénea de información

Sistema que entrega datos sobre una misma operación institucional, pero con formatos, alcances y niveles de detalle distintos. En una red institucional, puede tratarse de consolas en la nube, plataformas inalámbricas, gráficas históricas, archivos locales o registros validados por personal técnico.

Automatización

Reducción de tareas repetitivas mediante procesos programados que consultan fuentes, recuperan datos y preparan archivos intermedios. En este proyecto, automatizar no significó eliminar el criterio técnico, sino ordenar la información y liberar tiempo de revisión manteniendo validación humana cuando un indicador lo requería.

Normalización de datos

Proceso mediante el cual la información obtenida de distintas fuentes se convierte en una estructura común. Esta etapa permite comparar sedes, preparar indicadores homogéneos y evitar que el tablero dependa directamente del formato particular de cada herramienta.

Visualización ejecutiva

Presentación resumida de indicadores en un formato comprensible para seguimiento operativo y toma de decisiones. Su propósito no es reemplazar las consolas especializadas ni exponer configuraciones internas, sino ofrecer una primera lectura clara del estado general de la red.

2.2 MODELO CONCEPTUAL DE INTEGRACIÓN Y PROCESAMIENTO

A partir de los conceptos desarrollados en el apartado anterior, la solución puede entenderse como una capa de integración colocada sobre herramientas ya existentes. Esta capa no sustituye las plataformas de administración, sino que recupera información de ellas, la transforma y la presenta de manera común. Así, las consolas originales siguen disponibles para diagnósticos detallados, mientras que el tablero semanal funciona como una síntesis institucional.

La Tabla 1 resume las capas funcionales que intervienen en un sistema de este tipo. La separación por capas permite explicar qué componente aporta datos, cuál los procesa, dónde se normalizan y cómo se publican para consulta. Esta organización también ayuda a delimitar responsabilidades y a reducir el riesgo de exponer detalles técnicos innecesarios.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 28 - 46

Tabla 1

Hardware, software y comunicación por capa funcional

Capa funcional	*Hardware* o plataforma	*Software* o componente	Forma de comunicación
Fuentes de información	Puntos de acceso, *switches*, enlaces WAN y plataformas institucionales existentes	Aruba Central, Cisco Meraki Dashboard y estadísticas NOC/Cacti	API REST, consulta de gráficas históricas y captura asistida
Integración automatizada	Servidor Linux institucional	*Scripts* en Python, tareas programadas y archivos de configuración JSON	Consultas HTTPS hacia APIs y lectura de archivos intermedios
Normalización y ensamblado	Almacenamiento local del proyecto	Procesos Python de validación, conversión de unidades y generación de indicadores	Intercambio mediante archivos JSON crudos, normalizados y ensamblados
Visualización y publicación	Servidor web institucional	NGINX, HTML, JavaScript, hojas de estilo y certificado SSL	Publicación del tablero mediante HTTPS para consulta desde navegador

Nota. Se describen componentes generales para explicar la arquitectura sin exponer modelos, rutas, credenciales, direcciones ni parámetros internos.

La Figura 1 representa la arquitectura conceptual de la solución. En ella, se observa el paso desde sedes y fuentes de datos hacia una capa de integración, un proceso de normalización y una visualización ejecutiva.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 29 - 46

Figura 1

Arquitectura conceptual del sistema automatizado de monitoreo multi-sede

Nota. Figura de elaboración propia con apoyo de una herramienta de inteligencia artificial generativa para fines de representación visual. No contiene datos reales, rutas, direcciones ni identificadores sensibles.

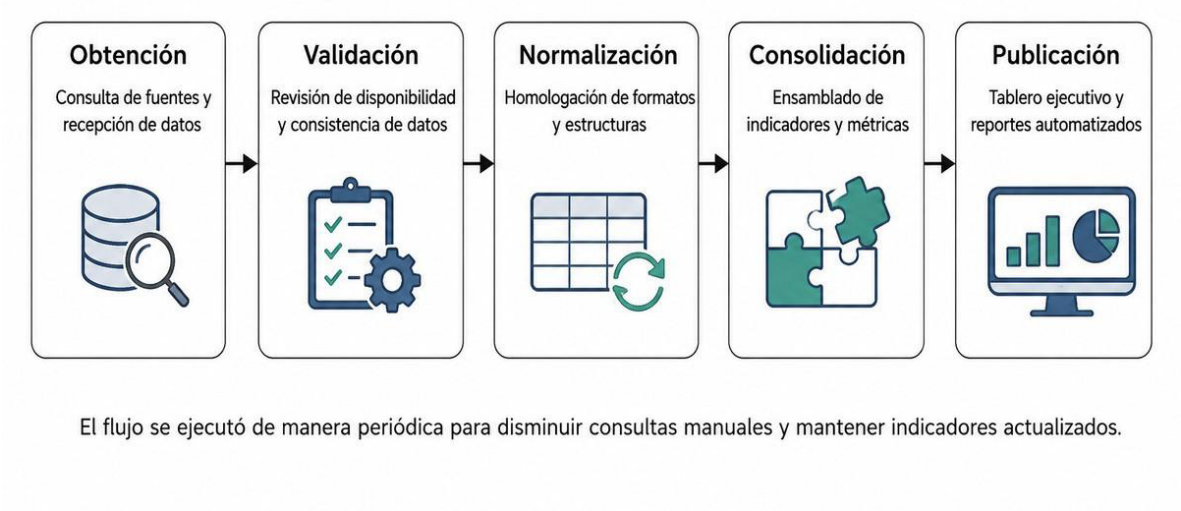
Esta representación muestra que el valor del sistema depende de articular fuentes existentes, procesos de integración y criterios de presentación comunes. Con ello, la arquitectura conceptual establece la base del flujo operativo que transforma una revisión dispersa en una consulta semanal organizada.

La Figura 2 complementa la arquitectura al mostrar el flujo general de procesamiento. La secuencia inicia con la identificación de fuentes y continúa con la extracción, validación, normalización, ensamblado, publicación y revisión operativa. Este flujo sirvió como guía para ordenar la implementación del sistema desarrollado.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 30 - 46

Figura 2

Flujo general de procesamiento de información en un sistema automatizado de monitoreo



Nota. Figura de elaboración propia con apoyo de una herramienta de inteligencia artificial generativa para fines de representación visual. No contiene datos reales ni información sensible.

Este flujo estableció que la confiabilidad del tablero dependía de separar obtención, validación, normalización y publicación, permitiendo revisar cada fuente sin afectar la lógica general del reporte semanal.

2.3 METODOLOGÍA DE DESARROLLO

La metodología se organizó en cuatro etapas: diseño, configuración, instalación y pruebas. Estas fases permitieron pasar de la identificación del problema a la puesta en operación de una aplicación funcional, conservando evidencia básica de las decisiones tomadas. La selección de una arquitectura modular se apoyó en trabajos recientes que destacan la conveniencia de desacoplar componentes de monitoreo para facilitar mantenimiento, crecimiento, integración de datos y generación automatizada de reportes (Khan y Khan, 2018; Quiñones-Cuenca *et al.*, 2025; Rafiq *et al.*, 2025).

La Tabla 2 muestra la relación entre cada etapa metodológica, su propósito general y su aplicación dentro del sistema. Esta tabla funciona como puente entre la explicación conceptual y el caso práctico que se describe en los apartados siguientes.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 31 - 46

Tabla 2

Etapas metodológicas utilizadas para el desarrollo del sistema

Etapa metodológica	Propósito general	Aplicación en el sistema
Diseño	Definir problema, sedes, indicadores y restricciones.	Cinco entornos, fuentes disponibles, métricas comunes y datos sensibles a excluir.
Configuración	Preparar parámetros, archivos y mecanismos de consulta.	JSON por fuente, extractores, datos crudos, datos normalizados y rutas de trabajo.
Instalación	Desplegar componentes y publicar resultados.	Servidor Linux, *scripts* en Python, NGINX, HTTPS y ejecución programada.
Pruebas	Validar datos, carga y correspondencia con fuentes.	Comparación contra consolas, revisión de archivos intermedios y ajustes al tablero.

Nota. Elaboración con base en la metodología seguida durante el diseño, configuración, instalación y pruebas del sistema automatizado de monitoreo.

Las etapas no se aplicaron de forma aislada. Cada una alimentó a la siguiente y, durante las pruebas, fue necesario regresar a etapas previas para ajustar archivos de configuración, validar métricas o corregir la forma en que una fuente entregaba información. Esta dinámica permitió mejorar el sistema sin cambiar su objetivo principal: integrar información de red dispersa y presentarla como un reporte semanal útil para seguimiento institucional.

2.4 APLICACIÓN DE LA METODOLOGÍA EN EL SISTEMA DEL IBUNAM

Una vez establecida la base conceptual y la metodología, el caso de implementación se describe siguiendo las mismas etapas. Esto permite observar cómo los conceptos de monitoreo multi-sede, automatización, normalización y visualización ejecutiva se tradujeron en decisiones concretas dentro del IBUNAM.

2.4.1 ETAPA DE DISEÑO: CONTEXTO, SEDES E INDICADORES

Durante la etapa de diseño, se delimitó el alcance institucional del sistema. Se consideraron cinco entornos de operación: el IBUNAM y el Pabellón Nacional de la Biodiversidad, ubicados en la Ciudad de México, así como la Estación La Posta en Colima, la Estación de Biología Los Tuxtlas en Veracruz y la Estación de Biología Chamela en Jalisco.

Esta distribución geográfica permitió dimensionar mejor el problema operativo. No se trataba únicamente de revisar equipos de red en un mismo edificio, sino de dar seguimiento a espacios con condiciones distintas de conectividad, administración, disponibilidad de datos y mecanismos de consulta. Por ello, desde el diseño se buscó una solución flexible, capaz de integrar información automática y también datos complementarios validados por personal técnico.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 32 - 46

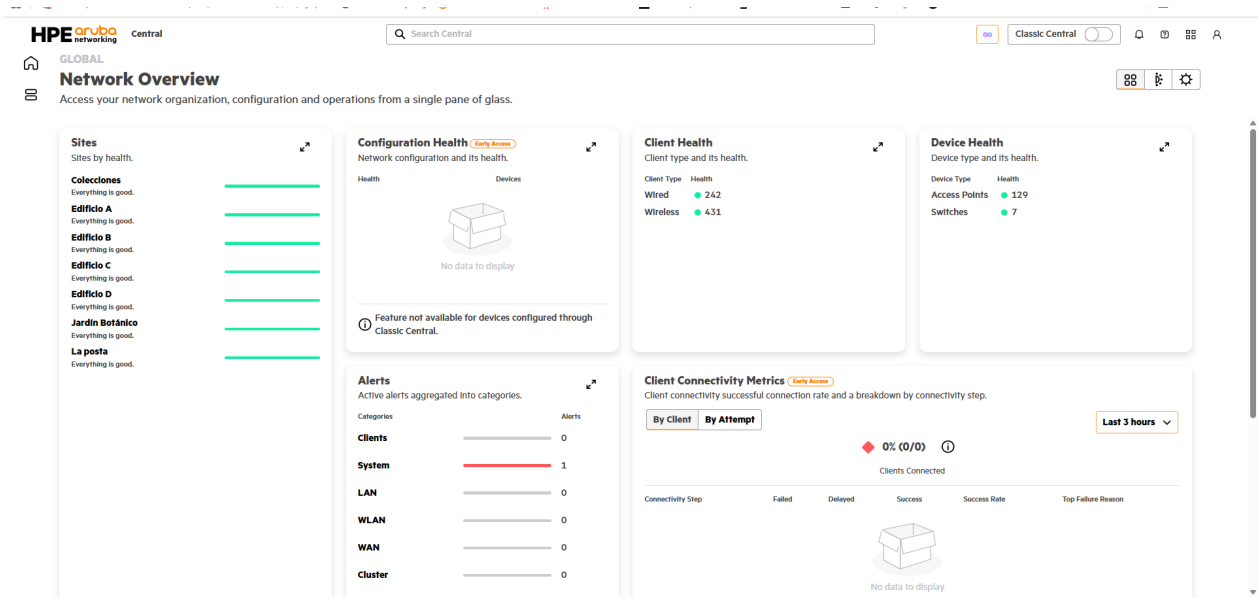
Antes de la implementación, la revisión del estado de la red se realizaba mediante consultas independientes. Para conocer el estado inalámbrico del IBUNAM, era necesario entrar a una plataforma; para revisar el Pabellón Nacional de la Biodiversidad, se consultaba otra consola; y para sedes foráneas, se recurría a gráficas históricas u observaciones operativas. Esta fragmentación dificultaba preparar una lectura semanal común.

También se definió que el reporte no debía mostrar información de configuración interna, direcciones sensibles, rutas, credenciales ni identificadores técnicos críticos. Esta restricción condicionó la forma de presentar resultados, porque el objetivo era ofrecer visibilidad operativa sin comprometer la seguridad de los servicios.

La primera fuente considerada fue Aruba Central, utilizada para la administración y supervisión de la infraestructura inalámbrica del IBUNAM. Desde esta plataforma, se obtuvieron indicadores relacionados con puntos de acceso, clientes conectados y estado operativo de la red inalámbrica. La Figura 3 muestra una vista de esta consola, donde se apreció la revisión por sitios, clientes y estado general de la red inalámbrica.

Figura 3

Vista de Aruba Central como fuente de indicadores inalámbricos institucionales

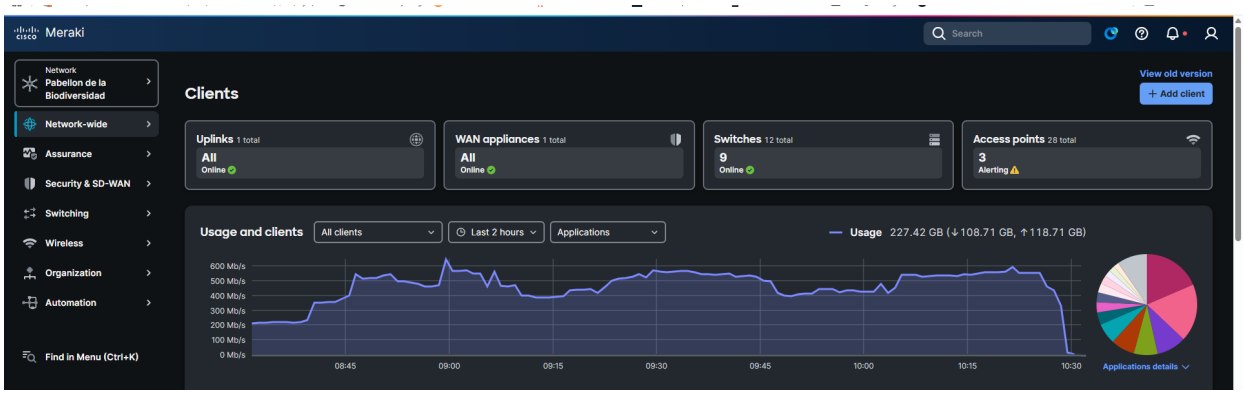


La segunda fuente fue Cisco Meraki Dashboard, empleada para el seguimiento de infraestructura del Pabellón Nacional de la Biodiversidad. Esta consola concentró información sobre equipos administrados desde la nube, clientes, conectividad y operación general de red. La Figura 4 presenta la vista operativa utilizada para consultar clientes, uso de red y estado de los equipos administrados desde la nube.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 33 - 46

Figura 4

Vista de Cisco Meraki Dashboard como fuente de indicadores del Pabellón Nacional de la Biodiversidad

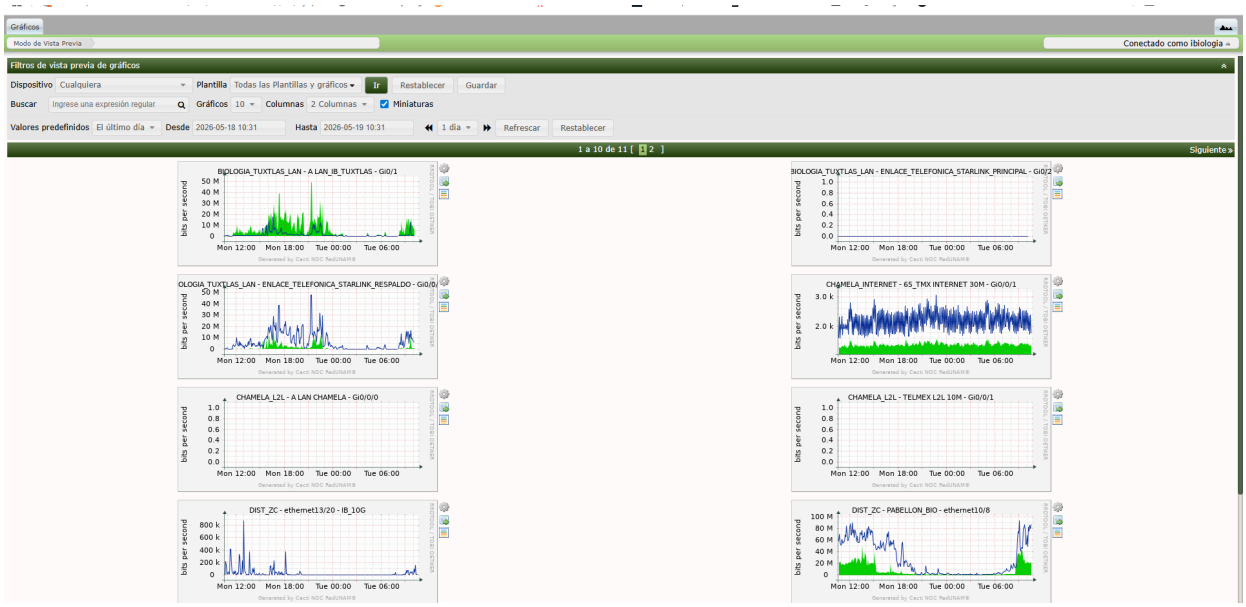


Nota. Se utiliza únicamente con fines descriptivos del flujo de monitoreo.

La tercera fuente correspondió al sistema de estadísticas de red del NOC, basado en gráficas históricas de comportamiento de enlaces. Esta plataforma permitió revisar tendencias de tráfico y disponibilidad observada en enlaces WAN, especialmente para sedes cuya información se evaluaba mediante comportamiento histórico. En la Figura 5 se muestra una representación de las gráficas utilizadas para complementar la captura de indicadores WAN.

Figura 5

Vista de gráficas históricas de enlaces en la plataforma NOC/Cacti



Nota. Se muestra una vista general de gráficas históricas de enlaces sin exponer credenciales.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 34 - 46

En conjunto, estas tres fuentes permitieron cubrir distintos niveles de la operación de red: la infraestructura inalámbrica institucional, los equipos administrados desde plataformas en la nube y el comportamiento histórico de enlaces. Su incorporación confirmó la necesidad de integrar información que originalmente se encontraba distribuida en consolas distintas, con alcances y formatos diferentes. Esta revisión inicial sirvió como base para definir qué datos podían automatizarse, cuáles requerían validación técnica y cómo debían organizarse para alimentar el reporte semanal.

La Tabla 3 resume las fuentes incorporadas y el tipo de datos que se aportaron al reporte semanal. La selección de estas plataformas respondió a su uso real dentro de la operación institucional y a la necesidad de reunir información que antes se revisaba de manera separada.

Tabla 3

Fuentes de información integradas en el reporte semanal

Fuente de información	Uso dentro de la operación	Indicadores aprovechados
Aruba Central	Administración de infraestructura inalámbrica del Instituto de Biología	Puntos de acceso, clientes conectados y estado operativo inalámbrico
Cisco Meraki Dashboard	Supervisión de infraestructura del Pabellón Nacional de la Biodiversidad	Dispositivos administrados, clientes, conectividad y estado general de red
Estadísticas NOC/Cacti	Seguimiento histórico de enlaces y tráfico entre sedes	Tendencias WAN, comportamiento de tráfico y disponibilidad observada
Captura asistida	Complemento para sedes sin integración automática completa	Valores operativos validados por el personal técnico
Aplicación local de reporte	Consolidación y publicación de indicadores semanales	Datos normalizados, históricos y visualización ejecutiva

Nota. Elaborada con base en las fuentes utilizadas durante la implementación del sistema.

La integración de estas fuentes confirmó que el sistema no debía depender de una única plataforma ni de un solo tipo de dato. Fue necesario combinar información automática, registros históricos y captura asistida para representar el estado semanal de la red. Con esta base, la etapa siguiente organizó archivos, parámetros y estructuras internas para transformar estos insumos en datos comparables.

2.4.2 ETAPA DE CONFIGURACIÓN: FUENTES, ARCHIVOS Y ESTRUCTURA INTERNA

En la etapa de configuración, se prepararon los archivos por fuente, los parámetros de consulta, las rutas internas de trabajo y las estructuras de salida. En esta fase, también se ajustaron los mecanismos de autenticación requeridos por las plataformas con API, así como los criterios para almacenar datos crudos y normalizados. La configuración se realizó de forma gradual, primero con una fuente y después con las demás, para reducir errores y facilitar la validación.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 35 - 46

La organización interna del proyecto se definió pensando en operación y mantenimiento, no sólo en desarrollo. Para ello, los archivos de configuración se separaron de los programas de extracción y los datos generados se guardaron en niveles distintos: información original recibida desde las plataformas, datos depurados, archivos normalizados e históricos, así como el archivo consolidado para la visualización.

Además de la descripción por directorio, se incorporó una vista simplificada del árbol del proyecto con la relación entre los componentes principales del sistema. Esta representación se muestra en la Figura 6 de manera general y no incluye rutas absolutas, credenciales ni parámetros internos de operación.

Figura 6

Estructura simplificada del sistema automatizado de monitoreo

```
[raíz del proyecto]/
├── config/
│   ├── sitios.json
│   ├── fuentes.json
│   ├── aruba_ibunam.json
│   ├── meraki_pabellon.json
│   └── pfsense_chamela_wan.json
├── extractors/
│   ├── extract_aruba.py
│   ├── extract_meraki.py
│   ├── extract_pfsense.py
│   └── capturar_wan_sedes.py
├── data/
│   ├── raw/
│   ├── normalized/
│   ├── assembled/
│   └── history/
├── assemblers/
│   └── assemble_reporte_semanal.py
├── utils/
│   ├── refresh_aruba_token.py
│   └── run_weekly_pipeline.sh
├── web/
│   ├── reporte_semanal_dashboard.html
│   ├── css/
│   └── js/
└── logs/
    ├── weekly_pipeline.log
    └── refresh_aruba_token.log
```

Nota. La estructura se muestra de forma simplificada para explicar la organización funcional del sistema; se omitieron rutas absolutas, credenciales, *tokens*, direcciones y parámetros de configuración.

En esta organización, los archivos de configuración definieron sedes y fuentes de datos; los extractores recuperaron información desde las plataformas integradas; los directorios de datos separaron información original, normalizada, ensamblada e histórica; el ensamblador generó el archivo consolidado del reporte; las utilerías apoyaron tareas programadas; el directorio web concentró los elementos publicados; y los registros permitieron revisar ejecuciones, errores y validaciones operativas.

La Tabla 4 resume la estructura general utilizada en el sistema. Por razones de seguridad, se presentan rutas relativas y funciones generales, sin incluir rutas absolutas del servidor, credenciales, identificadores internos ni archivos de configuración sensibles.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 36 - 46

Tabla 4

Organización estructural del sistema automatizado

Directorio o componente	Función principal	Descripción operativa
/config/	Configuración	Parámetros generales, sedes y fuentes; sin exponer credenciales.
/extractors/	Extracción	*Scripts* de consulta a plataformas y recuperación de métricas.
/data/raw/	Datos originales	Salidas preliminares obtenidas desde cada fuente
/data/normalized/	Normalización	Datos homologados para comparación y procesamiento común.
/data/assembled/	Consolidación	Indicadores finales usados por el tablero ejecutivo.
/utils/	Apoyo operativo	Tareas auxiliares, validaciones y ejecución calendarizada.
/web/	Publicación	Archivos HTML, JavaScript y recursos visuales del tablero.
/logs/	Registro	Evidencia básica de ejecuciones, errores y resultados.

Nota. Elaboración con base en la organización funcional del sistema desarrollado. Se omitieron rutas absolutas, credenciales y parámetros internos por criterios de confidencialidad operativa.

Esta organización separó las funciones principales y facilitó el mantenimiento del sistema. Al distinguir entre configuración, extracción, normalización, consolidación, publicación y registros, el proyecto quedó preparado para incorporar nuevas fuentes o ajustar procesos existentes sin modificar toda la estructura. Con esta base, la siguiente etapa consistió en instalar los componentes en el servidor institucional y habilitar la publicación segura del tablero.

2.4.3 ETAPA DE INSTALACIÓN Y PUBLICACIÓN

La etapa de instalación consistió en colocar los extractores, el ensamblador y el tablero web dentro de un servidor con sistema operativo Ubuntu Linux. Este entorno fue seleccionado por su estabilidad, facilidad para ejecutar procesos programados y compatibilidad con herramientas de automatización. Sobre esta base, se organizaron carpetas de configuración, *scripts* de extracción, datos crudos, información normalizada, históricos y archivos ensamblados para publicación.

Los procesos de obtención de información se desarrollaron principalmente mediante *scripts* en Python, apoyados por archivos de configuración en JSON y tareas de ejecución programada en el sistema operativo. Cada extractor tuvo una función específica: consultar una plataforma, recuperar métricas, validar la respuesta, convertir la información a una estructura común y almacenarla en archivos intermedios.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 37 - 46

En las plataformas administradas desde la nube, la consulta automática requirió atender aspectos propios de autenticación, vigencia de *tokens* y formatos de respuesta. Esta condición obligó a validar que las consultas no dependieran de una sesión abierta en navegador, sino de mecanismos controlados por la propia aplicación. Con esto, se redujo la intervención manual y se evitó que el reporte dependiera exclusivamente de capturas visuales realizadas por el personal técnico.

La información obtenida se almacenó en archivos JSON porque este formato facilitó el intercambio entre módulos y permitió revisar datos de manera sencilla durante las pruebas. En una primera etapa, se conservaron archivos crudos para validar qué entregaba cada fuente; después, se generaron archivos normalizados con campos comunes, unidades homogéneas y nombres consistentes. Finalmente, un proceso de ensamblado integró los indicadores por sede y preparó el archivo consumido por el tablero web.

La publicación de resultados fue realizada mediante un tablero desarrollado con HTML, JavaScript y hojas de estilo, servido desde NGINX. El motor de presentación quedó del lado del navegador: JavaScript leyó el archivo JSON consolidado y construyó dinámicamente tarjetas por sede, gráficas, semáforos de estado y observaciones operativas. Para proteger la consulta del sitio, se habilitó un certificado SSL expedido por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC), de modo que la página pudiera abrirse mediante HTTPS y la comunicación entre el navegador y el servidor quedara cifrada.

2.4.4 ETAPA DE PRUEBAS Y VALIDACIÓN OPERATIVA

La etapa de pruebas se concentró en revisar consistencia de datos, disponibilidad de archivos, carga del tablero, legibilidad de gráficas y congruencia entre lo observado en las plataformas originales y lo mostrado en el reporte consolidado. Cuando algún indicador no coincidía, se revisaba el extractor correspondiente, el archivo normalizado o la etapa de ensamblado. Este proceso permitió ajustar la aplicación antes de usarla como insumo de seguimiento semanal.

Cada extractor verificó que la fuente estuviera disponible y que los datos obtenidos tuvieran la estructura esperada. Cuando alguna fuente no entregaba información o presentaba diferencias con lo observado en su consola original, se revisaba el origen del dato antes de incorporarlo al reporte. Esta validación redujo inconsistencias y evitó publicar indicadores incompletos.

Las pruebas también permitieron detectar diferencias entre la información vista en las consolas y la información disponible para extracción automática. En algunos casos, los paneles gráficos mostraban datos agregados que no se obtenían de forma idéntica por API o que requerían transformaciones adicionales. Esta situación confirmó la necesidad de validar cada métrica antes de incorporarla al tablero y de documentar el origen de los indicadores.

Una vez publicado el reporte, el personal técnico podía comparar la información consolidada con las plataformas originales cuando era necesario. Esta revisión permitió validar que el tablero reflejara adecuadamente el estado semanal de las sedes y, al mismo tiempo, conservó la posibilidad de acudir a cada sistema especializado para diagnósticos más detallados.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 38 - 46

2.4.5 NORMALIZACIÓN DE DATOS

Para que los datos procedentes de plataformas distintas fueran comparables, no se utilizaron directamente los campos originales de cada sistema. Primero, se identificó la dimensión operativa de cada dato —por ejemplo, disponibilidad, conectividad WAN, operación inalámbrica, clientes conectados u observación técnica— y, después, se transformó a un registro común. Esta decisión evitó comparar valores que sólo tenían sentido dentro de la consola de origen y permitió que el tablero trabajara con indicadores homogéneos.

La regla lógica aplicada por los extractores puede resumirse como una función de normalización N (fuente, dato crudo, semana) que produce un registro normalizado con los campos: sede, fuente, indicador, valor, unidad, estado, método de obtención, fecha de consulta y observación operativa. El procesamiento siguió la siguiente secuencia: 1) validar que la fuente respondiera y que el dato tuviera estructura mínima; 2) asociar el dato con una sede institucional mediante un catálogo de configuración; 3) convertir unidades cuando fue necesario, por ejemplo, de bits por segundo, kilobits o megabits a Mbps; 4) homologar nombres y categorías de estado, como disponible, atención, crítico o sin dato; 5) marcar el origen como automático o asistido; y 6) guardar el resultado en archivos JSON normalizados para su ensamblado semanal. Esta lógica coincide con enfoques que ubican la agregación y normalización como una etapa previa necesaria para analizar datos heterogéneos en sistemas de monitoreo (Poltavtseva, 2020).

De esta manera, Aruba Central, Cisco Meraki Dashboard, las estadísticas NOC/Cacti y la captura asistida no se mezclaron como datos equivalentes sin revisión previa. Cada fuente aportó indicadores dentro de su propia dimensión operativa y el sistema sólo comparó métricas previamente transformadas a una estructura común. Cuando una fuente no entregó información completa, el registro se conservó como sin dato o como dato asistido, evitando presentar como automático un valor que requería validación técnica.

Esta formalización permitió resolver las diferencias entre los datos crudos de las plataformas y la información mostrada en sus paneles gráficos. El objetivo no fue replicar cada tablero propietario, sino extraer los elementos necesarios para construir una lectura institucional común, verificable y documentada, adecuada para el reporte semanal de estado de red.

2.5 VISUALIZACIÓN EJECUTIVA, SEGURIDAD Y ALCANCE

El tablero ejecutivo fue diseñado para responder una pregunta básica de operación: ¿cuál era el estado general de la red institucional durante la semana revisada? Para ello, se integraron tarjetas de resumen, gráficas de comportamiento, indicadores por sede y observaciones operativas. La intención no fue reemplazar los diagnósticos especializados, sino ofrecer una primera lectura clara para seguimiento y toma de decisiones.

La visualización separó la información por tipo de indicador: disponibilidad, conectividad, operación inalámbrica, tendencias y observaciones. Esta organización facilitó que el personal técnico identificara rápidamente dónde debía profundizar una revisión. Además, el tablero permitió distinguir entre datos obtenidos automáticamente y datos incorporados mediante captura asistida, lo cual fue importante para mantener transparencia sobre el origen de la información.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 39 - 46

La Figura 7 presenta una vista del tablero desarrollado para el reporte semanal de estado de red. En esta interfaz, se concentraron las fuentes de información, los sitios con datos, la obtención automática o manual de indicadores y el semáforo por sede. La captura fue utilizada para mostrar el resultado operativo del sistema y no como un inventario público de infraestructura.

Figura 7

Tablero ejecutivo desarrollado para el reporte semanal de estado de red

Nota.Se presenta con fines descriptivos y no expone credenciales ni rutas internas de configuración.

Asimismo, el tablero incorporó una herramienta de exportación a PDF, con el propósito de conservar una copia digital del estado del reporte en un momento determinado. Esta función permite generar registros documentales periódicos del tablero ejecutivo, útiles para fines de seguimiento, consulta histórica, respaldo institucional y comparación entre semanas. De esta manera, la información visualizada no quedó limitada a la consulta en pantalla, sino que pudo resguardarse como evidencia documental del comportamiento general de la red durante el periodo revisado.

Desde el inicio, se estableció que el reporte no debía convertirse en un inventario público de infraestructura. Por esa razón, se limitaron los datos visibles a indicadores generales y se evitó documentar configuraciones específicas, direcciones de red, credenciales, rutas internas o detalles que pudieran facilitar acciones indebidas. Esta decisión fue congruente con los lineamientos de confidencialidad aplicables a reportes técnicos sobre servicios TIC.

También se buscó que una falla parcial no impidiera la generación completa del reporte. Si una fuente no entregaba información en una ejecución determinada, el sistema debía permitir revisar el incidente sin

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 40 - 46

detener necesariamente el resto del flujo. Esta característica fue útil porque las plataformas dependían de servicios externos, conectividad y autenticaciones que podían presentar variaciones.

El sistema se concentró en indicadores operativos de red y no en el análisis profundo de seguridad, rendimiento de aplicaciones o monitoreo de servidores. Tampoco se planteó como plataforma de alertamiento en tiempo real. Su propósito fue construir un reporte semanal que permitiera observar tendencias, comparar sedes y disponer de una vista integrada de conectividad e infraestructura inalámbrica.

Esta delimitación permitió mantener el proyecto en un alcance viable. El valor del sistema estuvo en integrar información que ya existía, organizarla bajo un flujo común y presentarla de manera útil para seguimiento institucional. En consecuencia, la aplicación quedó preparada para crecer, pero sin perder el objetivo inicial de apoyar la supervisión operativa multi-sede.

3. RESULTADOS

La implementación permitió integrar en una misma vista información que antes se encontraba distribuida entre plataformas independientes y con diversidad tecnológica. Este resultado fue relevante porque la red institucional no se administra desde una sola herramienta: Aruba Central concentraba parte importante de la operación inalámbrica, Cisco Meraki aportaba información del Pabellón Nacional de la Biodiversidad y las gráficas del NOC permitían revisar comportamiento de enlaces. El tablero semanal reunió esos insumos en una lectura común.

El primer cambio observado fue la reducción de la fragmentación operativa. Antes del sistema, la preparación de un reporte requería abrir varias consolas, revisar gráficas, comparar datos y elaborar una síntesis manual. Después de la implementación, el personal técnico contó con un flujo que recuperó datos, los normalizó y los presentó en un formato homogéneo. Esto no eliminó la necesidad de revisar las plataformas originales cuando se requería diagnóstico detallado, pero sí facilitó la primera evaluación semanal.

El segundo resultado fue la incorporación explícita de cinco entornos institucionales distribuidos geográficamente: IBUNAM y Pabellón Nacional de la Biodiversidad en la Ciudad de México; Estación La Posta en Colima; Estación de Biología Los Tuxtlas en Veracruz; y Estación de Biología Chamela en Jalisco. Esta cobertura permitió observar la operación como un conjunto, no como revisiones aisladas de cada sede.

El tercer resultado fue la generación de una base histórica de indicadores. Al conservar reportes semanales, el sistema permitió revisar tendencias de conectividad, disponibilidad y comportamiento inalámbrico. Esta información será útil para identificar variaciones recurrentes, planear mantenimientos y justificar necesidades de mejora con datos organizados.

La existencia de un histórico también permitió comparar semanas sin depender de capturas aisladas o notas sueltas. Para las sedes foráneas, esta capacidad fue relevante porque los cambios de comportamiento en enlaces o servicios no siempre se observan en una sola revisión. Al acumular reportes semanales, el personal técnico pudo contar con una referencia más clara para distinguir entre una variación temporal y un patrón que requería seguimiento.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 41 - 46

Otro resultado fue la separación entre información técnica detallada e información ejecutiva. El sistema mostró estados, tendencias y observaciones, pero no expuso configuraciones internas ni identificadores críticos. Esta separación permitió comunicar el estado general de la operación sin comprometer la seguridad de la infraestructura.

Además, el reporte favoreció una comunicación más ordenada entre revisión técnica y seguimiento de coordinación. El personal especializado pudo conservar el acceso a las plataformas originales para análisis profundo, mientras que el tablero ofreció una síntesis útil para explicar el estado general de la red. Esta diferencia ayudó a evitar reportes excesivamente técnicos cuando sólo se requería una lectura operativa inicial.

Desde la operación diaria, el cambio también se observó en la forma de iniciar la atención de posibles incidentes. Antes de la implementación, en la red cableada se esperaba generalmente el reporte de una persona usuaria; a partir de esa notificación, se solicitaba la ubicación física, se identificaba el IDF correspondiente y se revisaba el nodo, el *switch* o el puerto asociado. En la red inalámbrica, ocurría algo semejante: después del reporte de baja señal o falta de conectividad, se ingresaba a la plataforma de la marca correspondiente para ubicar el punto de acceso o el *switch* relacionado. Con el tablero, la revisión inicial pasó a apoyarse en una visualización operativa continua y en indicadores consolidados, lo que permitió orientar con mayor rapidez la búsqueda del componente afectado. Esta mejora se considera principalmente una evidencia observacional del equipo técnico, complementada con las métricas de tiempo y ejecución que se presentan más adelante.

La Tabla 5 presenta una comparación entre el proceso previo y el proceso posterior a la implementación. El análisis mostró que el cambio más importante no fue únicamente tecnológico, sino organizativo: la información pasó de revisarse de forma dispersa a integrarse en una lectura semanal común.

Tabla 5

Comparación operativa antes y después de la implementación

Actividad	Antes de la implementación	Después de la implementación
Consulta de plataformas	Revisión independiente en consolas y gráficas separadas	Consulta consolidada desde el tablero semanal
Obtención de datos	Captura manual y validación caso por caso	Extracción automática y captura asistida cuando fue necesario
Seguimiento de sedes	Lecturas aisladas por ubicación o plataforma	Indicadores organizados por sede y tipo de servicio
Preparación de reportes	Integración manual de información dispersa	Ensamblado automatizado de datos normalizados
Comunicación operativa	Dependencia de explicaciones técnicas separadas	Visualización ejecutiva con indicadores resumidos
Protección de información	Riesgo de incluir detalles técnicos innecesarios	Presentación limitada a datos operativos no sensibles

Nota. La tabla fue elaborada con base en la comparación del proceso operativo antes y después de la implementación.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 42 - 46

Esta comparación muestra que la implementación modificó la forma de iniciar la revisión operativa de la red. Antes, el seguimiento dependía de consultas separadas e integración manual; después, el tablero permitió una primera lectura común por sede e indicador. Así, los resultados reflejaron una mejora técnica y una forma más ordenada de documentar, comunicar y dar seguimiento al estado semanal de la infraestructura.

Además de la comparación operativa, en la Tabla 6 se incorporaron métricas de referencia obtenidas durante una ejecución controlada del *pipeline* en el servidor institucional. Estas mediciones permitieron documentar recursos utilizados, duración de procesamiento, volumen de archivos JSON y beneficios estimados en la revisión inicial semanal.

Tabla 6

Métricas de operación y rendimiento incorporadas al análisis de resultados

Indicador	Resultado documentado	Interpretación operativa
Duración y estado del *pipeline*	66.99 segundos; código de salida 0; estado: éxito	La generación completa del flujo semanal se ejecutó correctamente en poco más de un minuto.
Uso de recursos del proceso medido	CPU: 88%; memoria máxima residente: 30,556 KB, aproximadamente 29.8 MB	El proceso utilizó recursos de CPU durante un periodo breve y mantuvo bajo consumo de memoria.
Evidencia JSON e histórico	205 archivos JSON; 1,104,998 bytes; semanas 2026-W22 a 2026-W25	El sistema conserva datos crudos, normalizados, ensamblados e históricos para comparación periódica.
Nivel de automatización de flujos	5 flujos automáticos y 2 asistidos; 71.4% automatizados	La mayor parte de la integración se resolvió mediante extracción automatizada, manteniendo captura asistida cuando la fuente lo requirió.
Tiempo de revisión inicial semanal	Antes: 45 a 60 minutos; después: 5 a 10 minutos	La consulta inicial se redujo aproximadamente entre 78% y 92%, de acuerdo con la estimación operativa del equipo técnico.
Cambio en la atención inicial	De una revisión reactiva por reporte de usuario a una revisión guiada por tablero	La herramienta permitió orientar con mayor rapidez la búsqueda por sede, IDF, *switch*, puerto o punto de acceso, sin sustituir el diagnóstico especializado.

Nota. Las métricas del pipeline corresponden a una ejecución controlada realizada el 21 de junio de 2026 en el servidor institucional. Los tiempos de revisión manual y con tablero son estimaciones operativas del equipo técnico, utilizadas como referencia para documentar la mejora en la consulta inicial semanal.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 43 - 46

Estos datos complementan las observaciones de mejora operativa del personal técnico. En conjunto, muestran que el sistema ordenó información dispersa, redujo el tiempo para iniciar la revisión semanal, mantuvo bajo consumo de recursos y dejó evidencia histórica para seguimiento institucional.

3.1 ANÁLISIS DE LOS RESULTADOS

Los resultados indicaron que la automatización aportó valor principalmente al ordenar el proceso de supervisión. En una red distribuida, el problema no siempre consiste en la ausencia de datos, sino en que esos datos se encuentran en sistemas distintos, con formatos diferentes y niveles variables de actualización. La aplicación desarrollada redujo esa dispersión y permitió que la primera revisión semanal partiera de una base común.

La incorporación de métricas cuantitativas no elimina el valor de la percepción técnica del personal responsable, pero sí permite respaldarla con evidencia mínima de operación. En este caso, las mediciones de ejecución del *pipeline* y la estimación de reducción de tiempo muestran que el tablero funcionó como apoyo para iniciar revisiones con mayor rapidez, mientras que la identificación precisa del incidente continuó dependiendo de las plataformas especializadas y de la experiencia del equipo de TIC.

La integración de plataformas también mostró que no todas las sedes podían tratarse igual. Las fuentes con API permitieron automatizar consultas de forma más directa, mientras que las fuentes basadas en gráficas o revisiones históricas requirieron una combinación de captura y validación. Esta diferencia no se consideró una falla del sistema, sino una condición real de operación que debía incorporarse al diseño.

El tablero ejecutivo mejoró la lectura inicial del estado de red porque tradujo información técnica en indicadores consultables. Esta transformación fue importante para apoyar tanto al personal técnico como a responsables de coordinación que requerían conocer el estado general sin entrar a cada plataforma. En consecuencia, el sistema fortaleció la comunicación operativa y facilitó el seguimiento institucional.

Además, la generación de datos históricos permitió que el reporte dejara de ser una fotografía aislada. Al conservar información semanal, se abrió la posibilidad de analizar tendencias, reconocer cambios en la demanda y anticipar necesidades de mantenimiento. Este componente será especialmente útil para sedes foráneas, donde la detección temprana de degradaciones puede reducir tiempos de atención.

En conjunto, la experiencia mostró que la integración automatizada no sustituyó el criterio del equipo técnico. Más bien, lo apoyó al reducir tareas repetitivas, ordenar la información y hacer visible el comportamiento general de la red. Las decisiones de diagnóstico y corrección siguieron dependiendo de especialistas, pero éstos contaron con información más accesible y mejor organizada.

El proyecto también evidenció que una solución de este tipo requiere mantenimiento operativo. Las APIs pueden cambiar, los permisos de consulta pueden modificarse y las plataformas externas pueden ajustar la forma en que entregan sus datos. Por ello, la aplicación no se concibió como un producto cerrado, sino como un sistema sujeto a revisión periódica, documentación interna y ajustes conforme evolucionen las herramientas de administración utilizadas por la institución.

Esta característica fue relevante porque el entorno de red universitario no permanece estático. La incorporación de nuevos puntos de acceso, cambios en enlaces, crecimiento de usuarios o incorporación de nuevas sedes pueden modificar los indicadores necesarios. La arquitectura modular permitió que

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 44 - 46

esos cambios pudieran atenderse mediante nuevos extractores, ajustes de normalización o ampliación del tablero, sin reconstruir todo el sistema desde el inicio y de forma gradual.

4. CONCLUSIONES

El sistema automatizado de monitoreo de red multi-sede cumplió el objetivo planteado al integrar información proveniente de plataformas heterogéneas, generar indicadores semanales y presentar una visualización ejecutiva para fortalecer la supervisión de servicios de comunicaciones en una institución universitaria. La implementación permitió pasar de una revisión fragmentada a un flujo común de obtención, normalización, ensamblado y publicación de datos.

La aportación principal consistió en construir una capa de integración sobre herramientas existentes. Esta decisión fue adecuada porque aprovechó plataformas ya utilizadas por el personal técnico, evitó duplicar funciones de administración y permitió avanzar sin sustituir la infraestructura de monitoreo disponible. En particular, la combinación de Aruba Central, Cisco Meraki, estadísticas del NOC y captura asistida permitió atender condiciones distintas entre sedes metropolitanas y foráneas.

La experiencia mostró que la distribución geográfica de las sedes no sólo representaba un dato contextual, sino una condición operativa que debía considerarse en el diseño. Supervisar espacios ubicados en Ciudad de México, Colima, Veracruz y Jalisco requería una herramienta capaz de reunir información de conectividad y disponibilidad sin depender de una revisión manual completa en cada plataforma.

Los resultados demostraron que la automatización mejoró la disponibilidad de información para seguimiento semanal, facilitó la comunicación técnica, permitió construir una base histórica útil para planeación y redujo el tiempo de consulta inicial de la red. El tablero ejecutivo no reemplazó las herramientas especializadas, pero sí ofreció una vista inicial integrada para identificar sedes, indicadores o tendencias que requerían mayor revisión.

Como continuidad del proyecto, convendría ampliar la automatización de fuentes que aún dependen de captura asistida, incorporar alertas tempranas para eventos relevantes y evaluar mecanismos de análisis predictivo a partir de históricos. También sería pertinente extender la cobertura hacia otros servicios tecnológicos, manteniendo el mismo criterio de mínima exposición de información sensible.

Finalmente, la implementación confirmó que una institución universitaria con sedes distribuidas puede fortalecer la gestión de su red mediante soluciones modulares, escalables y ajustadas a su operación real. El proyecto dejó una base técnica para continuar mejorando la supervisión, la continuidad y la planeación de los servicios digitales institucionales.

AGRADECIMIENTOS

Se agradece a la Unidad de Tecnologías de la Información y la Comunicación del Instituto de Biología de la UNAM, así como al personal de las sedes consideradas, por el apoyo brindado durante la validación operativa del sistema y la revisión de información necesaria para consolidar el reporte semanal.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 45 - 46

Declaración de contribución de autoría

Jorge Gerardo López Ibarra: Especialista en administración de redes, telecomunicaciones, seguridad informática y automatización de procesos TIC. Rol dentro del proyecto: diseño técnico, implementación operativa, integración de fuentes de información y desarrollo del sistema de reporte. Su contribución consistió en analizar la situación operativa del monitoreo de red institucional, identificar las fuentes de información disponibles y diseñar la arquitectura funcional del sistema automatizado. Participó directamente en la construcción de *scripts* de extracción, normalización y ensamblado de indicadores, así como en la integración de datos provenientes de plataformas de administración inalámbrica, seguridad perimetral, monitoreo remoto y captura asistida para sedes foráneas. También desarrolló y ajustó el tablero ejecutivo utilizado para presentar el reporte semanal, validó la consistencia de los datos obtenidos y documentó los criterios técnicos necesarios para proteger información sensible de infraestructura. Su participación permitió convertir una actividad de revisión dispersa en un proceso ordenado y repetible de supervisión institucional.

David Velázquez Portilla: Especialista en coordinación de servicios TIC, gestión operativa institucional y supervisión de infraestructura tecnológica. Rol dentro del proyecto: coordinación institucional, validación de necesidades operativas, seguimiento estratégico y revisión funcional del servicio implementado. Su contribución se centró en orientar el proyecto desde la perspectiva de las necesidades institucionales de supervisión y continuidad de servicios tecnológicos. Participó en la definición del alcance operativo, en la priorización de indicadores relevantes para el seguimiento de sedes y en la validación de que el reporte semanal fuera útil para actividades de coordinación técnica y comunicación institucional. También aportó criterios para que la solución mantuviera un equilibrio entre profundidad técnica, claridad ejecutiva y confidencialidad de información sensible. Su participación ayudó a vincular el desarrollo técnico con las necesidades reales de operación de la Unidad de Tecnologías de la Información y la Comunicación, fortaleciendo la pertinencia del sistema como herramienta de apoyo para la toma de decisiones.

REFERENCIAS

Boluda-Prieto, M., Sánchez, M., & Fernández, J. (2026). Resilient edge-to-cloud architecture with self-healing and self-correcting mechanisms for industrial data continuity. *Computers & Industrial Engineering*, *213*, 111795. https://doi.org/10.1016/j.cie.2025.111795

Espinel-Villalobos, R. I., Ardila-Triana, E., Zarate-Ceballos, H., & Ortiz-Triviño, J. E. (2022). Design and implementation of network monitoring system for campus infrastructure using software agents. *Ingeniería e Investigación*, *42*(1), e87564. https://doi.org/10.15446/ing.investig.v42n1.87564

Farahmand, H., Young, W. A., & Minsker, B. S. (2022). A network observability framework for sensor placement in infrastructure systems. *Reliability Engineering & System Safety*, *221*, 108363. https://doi.org/10.1016/j.ress.2022.108366

Khan, R., & Khan, S. U. (2018). Design and implementation of an automated network monitoring and reporting back system. *Journal of Industrial Information Integration*, *9*, 24-34. https://doi.org/10.1016/j.jii.2017.11.001

Lee, S., Levanti, K., & Kim, H. S. (2014). Network monitoring: Present and future. *Computer Networks*, *65*, 84-98. https://doi.org/10.1016/j.comnet.2014.03.007

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.181 **Vol. 4, Núm. 3.** julio-septiembre 2026, págs. 46 - 46

Poltavtseva, M. A. (2020). Heterogeneous data aggregation and normalization in information security monitoring and intrusion detection systems of large-scale industrial CPS. *Proceedings of the Institute for System Programming of the RAS*, *32*(5), 131-142. https://doi.org/10.15514/ISPRAS-2020-32(5)-10.

Quiñones-Cuenca, M., González, F., & Pérez, J. (2025). Architecture for Automated Real-Time Bidirectional Data Performance Analysis of LoRaWAN Networks. *Automation*, *6*(3), 38. https://doi.org/10.3390/automation6030038

Rafiq, A., Shakir, M. Z., Gray, D., Inglis, J., & Ferguson, F. (2025). AI and IoT-driven monitoring and visualisation for optimising MSP operations in multi-tenant networks: A modular approach using sensor data integration. *Sensors*, *25*(19), 6248. https://doi.org/10.3390/s25196248

Ta-Armart, W., & Savithi, C. (2026). Operational management of multi-vendor Wi-Fi networks in smart campus environments. *Technologies*, *14*(4), 204. https://doi.org/10.3390/technologies14040204

Witczak, D., Kelm, P., & Rybarczyk, A. (2024). Review of monitoring and control systems based on the Internet of Things. *Applied Sciences*, *14*(19), 8943. https://doi.org/10.3390/app14198943