CUADERNOS TÉCNICOS UNIVERSITARIOS DE LA DGTIC

ISSN-e: 3061-8096

Vol. 3, Núm. 3. julio-septiembre 2025

DOI:10.22201/dgtic.30618096e.2025.3.3

DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Cuadernos Técnicos Universitarios de la DGTIC

DOI: 10.22201/dgtic.30618096e.2025.3.3

Vol. 3, Núm. 3. julio-septiembre 2025

Cuadernos Técnicos Universitarios de la DGTIC

DOI: 10.22201/dgtic.30618096e.2025.3.3

Vol. 3, Núm. 3. julio-septiembre 2025

CUADERNOS TÉCNICOS UNIVERSITARIOS DE LA DGTIC

Comité Editorial de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Para citar un reporte técnico de la obra: Apellidos 1 Apellidos 2, Iniciales nombres. (2025). Título del reporte técnico. *Cuadernos Técnicos Universitarios de la DGTIC, 3* (3), páginas (N1-N2).

Cuadernos Técnicos Universitarios de la DGTIC

DOI: 10.22201/dgtic.30618096e.2025.3.3

Vol. 3, Núm. 3. julio-septiembre 2025

CUADERNOS TÉCNICOS UNIVERSITARIOS DE LA DGTIC, Año 3, No. 3, julio-septiembre 2025, es una publicación trimestral editada por la Universidad Nacional Autónoma de México, Ciudad Universitaria, Alcaldía Coyoacán, C.P. 04510, Ciudad de México, a través de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Circuito Exterior s/n, frente a la Facultad de Contaduría y Administración, Ciudad Universitaria, Alcaldía Coyoacán, C.P. 04510, Tel. (55) 5622 8502 y 5622 8354, URL: https://cuadernos.tic.unam.mx, correo electrónico cuadernostecnicos-dgtic@unam.mx, Editor responsable: Dr. Héctor Benítez Pérez. Certificado de Reserva de Derechos al Uso Exclusivo de Título: 04-2023-100610042700-102, ISSN-e: 3061-8096, ambos otorgados por el Instituto Nacional del Derecho de Autor. Dra. Marcela J. Peñaloza Báez, responsable de la última actualización de este número, Circuito Exterior s/n, frente a la Facultad de Contaduría y Administración, Ciudad Universitaria, Alcaldía Coyoacán, C.P. 04510, Ciudad de México. Fecha de la última modificación, 13 de agosto de 2025.

Cuadernos Técnicos Universitarios de la DGTIC

DOI: 10.22201/dgtic.30618096e.2025.3.3

Vol. 3, Núm. 3. julio-septiembre 2025

COLABORADORES

Dirección General de Publicaciones y Fomento Editorial a través de Socorro Venegas Pérez, Directora General • Guillermo Chávez Sánchez, Subdirector de Revistas Académicas y Publicaciones Digitales • Lilia Nataly Vaca Tapia, Jefa de Gestión de Revistas Académicas • Jorge Pérez García, Jefe del Departamento de Soporte Técnico de Sistemas Editoriales • Juan Manuel Rodríguez Martínez, Jefe de Desarrollo • Victor Daniel Haro Gómez, Diseñador web • Jaqueline Segura Bautista, Gestión de recursos.

Dirección General de Cómputo y de Tecnologías de Información y Comunicación a través de Ana Yuri Ramírez Molina, Directora de Colaboración y Vinculación • Juan Manuel Castillejos Reyes, Líder de proyecto de Soporte Técnico • Alberto González Guízar, Infraestructura y software • José Othoniel Chamú Arias, Servidores y bases de datos • Miguel Ángel Islas Flores, Diseño gráfico y editorial • Jonathan Cedillo Castro, Maquetador • Jorge Alberto Colín Rojas, Responsable de biblioteca.

Cuadernos Técnicos Universitarios de la DGTIC

DOI: 10.22201/dgtic.30618096e.2025.3.3

Vol. 3, Núm. 3. julio-septiembre 2025

Cuadernos Técnicos Universitarios de la DGTIC

DOI: 10.22201/dgtic.30618096e.2025.3.3 **Vol. 3, Núm. 3.** julio-septiembre 2025

CONTENIDO

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113

Vol. 3, Núm. 3. julio-septiembre 2025, págs. 8 - 15

Migración de datos del TICómetro a Superset: optimizando el análisis de habilidades TIC

Información del reporte:

Para citar este reporte técnico:

Mejía Argueta, M.A.G. (2025). Migración de datos del TICómetro a Superset: optimizando el análisis de habilidades TIC. *Cuadernos Técnicos Universitarios de la DGTIC, 3* (3) página(8 - 15). https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113

Miguel Angel Germán Mejía Argueta

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Universidad Nacional Autónoma de México

miguel.argueta@unam.mx

ORCID: 0000-0001-8904-8905

Resumen

El TICómetro es una herramienta de evaluación diagnóstica que permite analizar las habilidades en el uso de las Tecnologías de la Información y Comunicación (TIC) de los estudiantes de la Universidad Nacional Autónoma de México. Desde su implementación en 2012, los datos obtenidos se almacenaron en la base de datos de Moodle, plataforma utilizada para la aplicación del instrumento. El trabajo técnico que se realizó consistió en migrar los datos del TICómetro hacia una nueva fuente de datos externa estructurada para su análisis en Apache Superset, con el propósito de facilitar su transformación, limpieza, normalización y carga, de acuerdo con las necesidades analíticas del proyecto Migración de datos del TICómetro a Superset. Para la migración se emplearon Python y Google Colaboratory Notebooks, herramientas utilizadas para automatizar la extracción, transformación y carga (ETL) de los datos, así como para garantizar su integridad y consistencia. El proceso consideró las diferencias estructurales entre versiones de Moodle y se orientó a obtener una base de datos PostgreSQL optimizada para su conexión con Superset. Como resultado, se generaron los esquemas técnicos de datos y scripts automatizados que permiten integrar y consultar la información del TICómetro en Superset. Estos productos sientan la base técnica para la creación de reportes interactivos en el proyecto *Sitio de Resultados del TICómetro*.

Palabras clave:

TICómetro, migración de datos, Moodle, Apache Superset, habilidades TIC.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 9 - 15

Abstract

The TICómetro is a diagnostic assessment tool designed to analyze the Information and Communication Technology (ICT) skills of students at the Universidad Nacional Autónoma de México (UNAM). Since its implementation in 2012, the data collected has been stored in the Moodle database, which supports the administration of the instrument. The technical work realized consisted of migrating the TICometer data to a new external data source structured for analysis in Apache Superset, with the purpose of facilitating its transformation, cleaning, normalization and loading, according to the analytical needs of the Migración de datos del TICómetro a Superset project. For the migration, Python and Google Colaboratory Notebooks were employed to automate the extraction, transformation and loading (ETL) processes, ensuring data integrity and consistency. The procedure addressed structural differences among Moodle versions and resulted in a PostgreSQL database optimized for Superset connectivity. As an outcome, the project produced technical data schemes and automated scripts that enable the integration and querying of TICómetro information within Superset. These outputs establish the foundation for developing interactive reports as part of the Sitio de Resultados del TICómetro project.

Keywords:

Performance testing, automation scripts, LimeSurvey, Selenium WebDriver Sampler, JMeter.

1. INTRODUCCIÓN

El TICómetro (Dirección General de Cómputo y de Tecnologías de Información y Comunicación [DGTIC], 2025) es un instrumento de evaluación diagnóstica que permite analizar las habilidades en el uso de las Tecnologías de la Información y Comunicación (TIC) de los estudiantes de nuevo ingreso a la Universidad Nacional Autónoma de México. Desde su implementación en 2012, utiliza la plataforma Moodle (Moodle, 2025) como entorno tecnológico para la aplicación del cuestionario y el registro de resultados, y aprovecha su capacidad para gestionar actividades de evaluación en línea y generar estadísticas sobre el desempeño de los participantes. Su base pedagógica socio-constructivista, según Devi y Aparna (2020), respalda el trabajo del TICómetro al promover un aprendizaje centrado en la interacción.

Apache Superset (Sanz, 2023) es una herramienta de análisis y visualización de datos de código abierto que permite crear tableros interactivos y personalizar visualizaciones a partir de diversas fuentes de información. La migración de los datos del TICómetro a esta plataforma ofrece una estructura homogénea y escalable que facilita el análisis comparativo de habilidades digitales a lo largo de distintos periodos académicos.

A partir de las migraciones para la integración de los datos del TICómetro en Apache Superset (Apache Superset, 2024) realizadas entre 2022 y 2024, se contaba ya con una estructura de base de datos diseñada y funcional, así como con visualizaciones disponibles en el sitio institucional https://ticometro.unam.mx/resultados/. Este antecedente técnico permitió contar con un punto de partida consolidado para ampliar el proceso de migración hacia los datos históricos correspondientes al periodo 2012–2021, realizado entre septiembre y diciembre de 2024, previo a la etapa de visualización. Los *scripts* que me fueron proporcionados en la Dirección de Innovación en Tecnologías para la Educación (DITE) de la DGTIC[1], los

1 Con el apoyo de Javier Rodrigo Díaz Espinosa, jefe del Departamento de Desarrollo Tecnológico para la Educación.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 10 - 15

cuales habían sido utilizados en las migraciones previas, junto con una copia de una máquina virtual y un sistema de pruebas, fueron elementos fundamentales para la comprensión del proceso y la correcta ejecución de la nueva migración.

La necesidad de realizar la migración de los datos históricos del TICómetro respondió a la heterogeneidad de las versiones de Moodle empleadas entre 2012 y 2021, cuyas diferencias estructurales en los modelos de datos dificultaban la aplicación directa de los procesos de extracción, transformación y carga (ETL) desarrollados para los años más recientes. Cada versión de Moodle presenta variaciones en el diseño de tablas, nombres de campos y relaciones entre datos, lo que hizo necesario desarrollar un proceso técnico de migración adaptado a cada estructura. Este desafío de ETL heterogéneo constituyó el núcleo del trabajo técnico aquí descrito.

En este contexto, el presente reporte se enfoca exclusivamente en las actividades técnicas relacionadas con la migración de los datos de Moodle hacia la fuente de datos empleada por Apache Superset. Dichas actividades comprendieron la extracción de datos desde las distintas versiones de Moodle, su limpieza y normalización, así como su carga en una base de datos PostgreSQL ya existente y estructurada para su uso con Superset. Es importante destacar que la estructura de esta base de datos no fue creada nuevamente para este proyecto, sino que se reutilizó y adaptó para integrar los datos históricos de los años 2012 a 2021.

El desarrollo técnico incluyó la creación de *scripts* propios escritos en Python, ejecutados en Google Colaboratory Notebooks, que permitieron automatizar el proceso ETL y garantizar la consistencia de los datos. Aunque los *scripts* originales de los años 2022–2024 que me fueron proporcionados por la DITE sirvieron como referencia metodológica, las diferencias entre las versiones antiguas de Moodle y los cambios en la organización de los datos requirieron la reescritura completa de los procedimientos y la optimización de su desempeño mediante bibliotecas de análisis de datos y control de errores.

Entre los productos técnicos derivados de este proceso se encuentran:

1. Los scripts en Python desarrollados para la migración de los datos del periodo 2012–2021.
2. Los archivos Excel con los resultados anuales correspondientes a los niveles de bachillerato y licenciatura.
3. La normalización de catálogos institucionales y académicos que garantizó la uniformidad de los registros.
4. La documentación metodológica del proceso de migración y las verificaciones de integridad de datos.

El objetivo del trabajo técnico es llevar a cabo el proceso de migración de los datos del TICómetro, almacenados en Moodle, hacia una nueva fuente de datos estructurada para su análisis en Apache Superset, con el propósito de facilitar su transformación, limpieza, normalización y carga, de acuerdo con las necesidades analíticas del proyecto Migración de datos del TICómetro a Superset. Su importancia radica en la consolidación de los datos históricos del TICómetro dentro del mismo entorno analítico empleado por las versiones recientes, lo que brinda una base técnica unificada que fortalece la capacidad institucional para generar reportes y análisis longitudinales sobre las competencias digitales de los estudiantes.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 11 - 15

2. DESARROLLO TÉCNICO

La migración de los datos del TICómetro (DGTIC, 2012) a Apache Superset facilita el análisis de las habilidades digitales de los estudiantes de nuevo ingreso de la UNAM al consolidar, por primera vez, datos homogéneos con esquemas unificados para los años migrados (2012–2021); permite disponer de una fuente de datos estructurada y consistente que servirá como base para la futura visualización dinámica de resultados en el sitio https://ticometro.unam.mx/resultados/. La integración en Superset (Apache Superset, 2024) favorece la interoperabilidad de los datos, la consulta transversal por periodo académico y la preparación para la siguiente etapa del proyecto: *Sitio de Resultados del TICómetro*.

El proceso técnico presentado en este documento forma la primera parte del proyecto institucional *Sitio de Resultados del TICómetro*, desarrollado por la DGTIC. Entre 2022 y 2024 se realizaron las primeras migraciones correspondientes a dichos años en la DITE[2]. A partir de los *scripts* iniciales de migración y una máquina virtual para pruebas que me fueron proporcionados, se revisó también el diseño del modelo de datos en Superset[3] y otros elementos como el desarrollo web, la integración del sitio de resultados, el manual de procedimientos y la transferencia de conocimientos sobre la creación de *dashboards*[4]; estos elementos son fundamentales para la continuidad del proyecto hacia la fase web.

El presente trabajo amplía dicho proceso al incorporar los datos históricos de 2012 a 2021, un desafío técnico que requirió adaptar el proceso de extracción, transformación y carga (ETL) a múltiples versiones de Moodle con modelos de datos heterogéneos. La Tabla 1 resume las versiones de Moodle utilizadas, y muestra al menos seis versiones distintas que debieron ajustarse para generar una fuente de datos homogénea compatible con Superset.

2 Javier Rodrigo Díaz Espinosa, jefe del Departamento de Desarrollo Tecnológico para la Educación, coordinó estas actividades.

3 Realizado por Cristian Ricardo Ortega Ramírez, colaborador de la DITE.

4 Contribuciones de José Larios Delgado y de César Ordóñez Rodríguez.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113 Vol. 3, Núm. 3. julio-septiembre 2025, págs. 12 - 15

Tabla 1

Evolución de versiones de Moodle utilizadas entre 2012 y 2021

Año	Versión	Build
2012	1.9.19+ (Build: 20120726)	Estructura inicial basada en tablas planas, sin normalización; campos como *description* y *assignmenttype*.
2013	2.4.4 (Build: 20130513)	Renombrado de *description* --> *intro* y adición de *introformat*; nueva *collation* utf8_unicode_ci.
2015-2016	2.6.11 (Build: 20150511)	Cambios en tablas *mdl_user* y *mdl_quiz_attempts*; incorporación de campos *modifided* y *timelimit*.
2017-2018	3.2.9 (Build: 20180517)	Reestructuración de *mdl_question_attempts*; nuevos identificadores en tablas de usuarios.
2019-2021	3.3.9+ (Build: 20190201)	Consolidación de esquemas; adopción definitiva de UTF-8 universal.

Estas diferencias motivaron a la redefinición de las consultas SQL y las rutinas de transformación de datos, particularmente en los campos de texto, identificadores y tipos de relación. El análisis de las estructuras mostró que las versiones 1.9.x y 2.4.x requerían mayor intervención debido a la falta de consistencia en las claves primarias y foráneas, mientras que las versiones posteriores permitieron automatizar parcialmente la extracción.

El proceso ETL se ejecutó bajo un enfoque modular y reproducible en el entorno de Google Colaboratory Notebooks, para garantizar trazabilidad, seguridad y control de versiones. Los datos del TICómetro ya estaban anonimizados desde su origen, antes de su exportación desde Moodle, en cumplimiento con la normatividad universitaria sobre protección de datos.

Los volúmenes de información migrados permiten dimensionar la magnitud del trabajo técnico realizado. En el nivel bachillerato, la tabla fac_evaluación acumuló entre 22,917 y 33,620 registros anuales, con un promedio de 31,000 registros por año. En el nivel licenciatura, a partir de 2013, se registraron volúmenes entre 826 y 15,709 evaluaciones anuales, lo que representa en total más de 300,000 registros migrados. En la tabla población_institución, que contiene la información institucional y de grupos, se integraron 14 planteles de bachillerato y hasta 482 registros de grupos de universitarios por año en licenciatura, según el periodo correspondiente.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 13 - 15

El análisis de las diferencias estructurales entre versiones de Moodle permitió desarrollar una estrategia de migración flexible. Las modificaciones incluyeron la detección de cambios de tipo de dato (por ejemplo, de varchar a text) y ajustes de collation a utf8_unicode_ci y renombrado de campos (como description - intro), lo que requirió reestructurar las consultas de extracción y los mapeos de transformación. Esta labor garantizó que los datos migraran sin pérdida ni duplicidad y bajo un modelo de datos unificado en Superset.

El modelo de datos proporcionado en Superset sigue un diseño relacional y permite una estructura analítica uniforme y escalable para futuros tableros interactivos; fue diseñado originalmente por el equipo de colaboradores del proyecto *Sitio de Resultados del TICómetro*, con las siguientes tablas:

- dim_cinta: niveles de competencia TIC (cinturón blanco a negro).
- dim_fecha: control temporal del año y periodo de aplicación.
- dim_institución: dependencias, planteles y facultades.
- dim_sexo: variable demográfica normalizada.
- fac_evaluación: tabla de hechos con los resultados individuales por usuario y nivel.
- población_institución: totales agregados por dependencia.

Se incorporaron mejoras al proceso ETL modificado respecto a las migraciones anteriores, tales como:

1. Entorno de trabajo: configuración del entorno en Google Colab e importación de las bibliotecas *pandas*, *numpy*, *psycopg*, *sqlalchemy*, *os*, *re*, *datetime* y *google.colab*, con el fin de automatizar la conexión, limpieza y carga de datos.
2. Extracción (E): conexión directa a las bases de datos Moodle mediante *psycopg* y ejecución de consultas SQL con filtros por fecha y estado de finalización (*qa.state='finished'*).
3. Transformación (T): creación de funciones de categorización (*categorize_cinta*, *nivel*, *convert_to_list*) para clasificar, limpiar y reestructurar los datos.
4. Procesamiento diferenciado: tratamiento individual de los datos de los niveles bachillerato y licenciatura, transformando respuestas en formato largo (*long format*) a formato ancho (*wide format*) y aplicando codificación *one-hot* para preguntas de opción múltiple.
5. Carga (L): modelado en base de datos PostgreSQL bajo esquema de estrella, creación de tablas con to_sql() y almacenamiento de datos agregados.
6. Exportación: generación de reportes en Excel por nivel educativo y año para su validación por las dependencias académicas.

En total, el proceso de migración se ejecutó en un solo archivo de código en Google Colaboratory, lo que permitió reproducir la operación de principio a fin. La automatización de rutinas y la limpieza de datos incrementaron la eficiencia del proceso y redujeron el riesgo de errores manuales.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 14 - 15

La migración de datos entre múltiples versiones de Moodle hacia un modelo homogéneo en Superset representa una valiosa optimización técnica: homogeneiza los esquemas, reduce la fragmentación de los datos, mejora la capacidad de análisis comparativo interanual y sienta las bases para la generación de tableros analíticos que integrarán todos los años históricos del TICómetro en un mismo entorno visual. Este tema será motivo de un trabajo técnico posterior, enfocado en la etapa de elaboración y publicación de los *dashboards*.

2.1 METODOLOGÍA

A continuación se describen los pasos realizados durante el proceso de migración de los datos del TICómetro, correspondientes al periodo 2012–2021, ejecutado entre septiembre de 2024 y diciembre de 2024. Este procedimiento tuvo como objetivo trasladar la información almacenada en las bases de datos Moodle hacia los esquemas de la fuente de datos utilizada por Superset, en formato PostgreSQL, para su posterior análisis e integración en el proyecto *Sitio de Resultados del TICómetro*.

Los datos se extrajeron desde un servidor de respaldo proporcionado por la DITE de la DGTIC[5]. La extracción se realizó por año, para lo cual se emplearon consultas SQL directas mediante la biblioteca *psycopg* de Python. Para garantizar la trazabilidad y control de versiones, se desarrolló un archivo independiente de Google Colaboratory Notebook por cada año migrado desde 2012 hasta 2021.

Cabe recalcar que los datos del TICómetro ya se encontraban anonimizados desde su origen, es decir, antes de su exportación desde Moodle, en cumplimiento con la normatividad universitaria sobre protección de datos académicos.

El proceso de migración se estructuró conforme al enfoque ETL (Extracción, Transformación y Carga), con la siguiente secuencia de pasos y herramientas empleadas en cada fase de la Tabla 2:

5 Con el apoyo de Javier Rodrigo Díaz Espinosa, jefe del Departamento de Desarrollo Tecnológico para la Educación.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 15 - 15

Tabla 2

Herramientas utilizadas en cada fase del proceso ETL

Fase	Herramientas utilizadas	Función
Extracción	Python (*psycopg, sqlalchemy*), Google Colab	Conexión directa al servidor Moodle de respaldo y ejecución de consultas SQL para cada año.
Transformación	*pandas, numpy, re, datetime*	Limpieza, categorización y normalización de los datos; conversión de estructuras y formatos.
Carga	*sqlalchemy*, método *to_sql()*	Inserción de datos procesados a la base PostgreSQL (fuente de datos utilizada por Superset).
Validación y reporte	*pandas, openpyxl*	Generación de reportes Excel y verificación de integridad de los datos migrados.
Control y respaldo	Google Drive (Colab)	Almacenamiento de archivos de salida y registro de bitácoras de ejecución.

Los pasos realizados entre los meses de septiembre y diciembre de 2024 fueron:

1. Respaldo y conexión inicial: se estableció conexión con la base de datos Moodle de respaldo, definiendo los rangos de fechas de extracción y ejecutando las consultas SQL a través de *psycopg*.
2. Extracción de usuarios y respuestas: se obtuvieron datos de las tablas *mdl_user*, *mdl_quiz_attempts* y *mdl_question_attempts*, filtrando intentos finalizados y transformando los resultados a estructuras manejables mediante *pandas*.
3. Transformación de datos: se aplicaron funciones para categorizar resultados, normalizar nombres de instituciones, limpiar duplicados y transformar los formatos de tiempo.
4. Procesamiento diferenciado por nivel educativo: se separaron los conjuntos de datos de bachillerato y licenciatura, y se ajustaron los esquemas y campos de cada uno de acuerdo con las versiones de Moodle correspondientes.
5. Carga en la fuente de datos utilizada por Superset: los datos limpios se insertaron en la base PostgreSQL, respetando la estructura de seis tablas (dim_cinta, dim_fecha, dim_institución, dim_sexo, fac_evaluación y población_institución).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 15A - 15

Con el propósito de conservar la coherencia visual y estructural con las publicaciones previas del proyecto, la generación de reportes en Excel se realizó siguiendo el formato de los reportes oficiales del TICómetro[1]. Posteriormente, en el año 2025 las actividades se centraron en la consolidación y verificación de los datos históricos migrados y en la preparación de los *dashboards* interactivos que integrarán los resultados de los años 2012 a 2021 con los datos más recientes. Cuando dichos *dashboards* estén disponibles públicamente en el sitio oficial, se habrá completado la segunda fase del proyecto *Sitio de Resultados del TICómetro*.

3. RESULTADOS

La migración de los datos del TICómetro correspondientes al periodo 2012–2021 permitió consolidar una fuente de datos histórica bajo un mismo modelo analítico, compatible con la herramienta Apache Superset. En total, se procesaron y migraron más de 600,000 registros, provenientes de los niveles de bachillerato y licenciatura, que incluyeron información demográfica, académica y de desempeño en las evaluaciones de habilidades digitales.

El proceso de migración culminó con la carga exitosa de los datos en los esquemas de la fuente de datos utilizada por Superset, con independencia por año. Esta organización estructural permite mantener la integridad de los datos y evitar conflictos derivados de las diferencias entre versiones de Moodle. Cada año cuenta con su propio esquema, lo que facilita las operaciones de comparación interanual y garantiza la trazabilidad de las transformaciones realizadas durante el proceso ETL.

En términos de volumen, las tablas principales migradas fueron fac_evaluación, que concentra las respuestas individuales de los estudiantes, y poblacion_institución, que contiene la información de los planteles, facultades y grupos participantes. La Tabla 3 resume el volumen de registros migrados por nivel educativo y año en la tabla fac_evaluación.

1 Disponibles en https://educatic.unam.mx/publicaciones/ticometro/index.html

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 15B - 15

Tabla 3

Registros migrados en la tabla fac_evaluacion por año y nivel académico

Año	Bachillerato (respuestas individuales)	Licenciatura (respuestas individuales)
2012	22 917	-
2013	31 949	826
2014	32 024	3 434
2015	33 385	5 047
2016	33 272	11 300
2017	33 620	12 412
2018	31 019	12 058
2019	32 000	14 455
2020	31 746	14 009
2021	28 984	15 709

La creación de esquemas independientes por año se justifica por las diferencias estructurales entre las versiones de Moodle de las que provienen los datos, para evitar conflictos de integridad y garantizar la compatibilidad con los modelos de datos empleados en cada periodo. Este enfoque permite conservar la trazabilidad de las modificaciones y facilita el mantenimiento en futuras actualizaciones.

En cuanto al archivo de preguntas, su actualización anual impacta de manera significativa la coherencia y calidad analítica de los datos; se compone de los reactivos demográficos, de habilidades y de conocimiento sobre el uso de TIC aplicados en Moodle, posteriormente migrados a Superset. Dado que el cuestionario cambia cada año, la gestión y estandarización del archivo de preguntas resultan fundamentales para mantener la continuidad de las métricas y posibilitar el análisis longitudinal de los resultados entre generaciones de estudiantes.

La migración también mejoró la consistencia de los datos históricos al actualizar los catálogos de dependencias participantes y normalizar la codificación de instituciones, modalidades y grupos. Estos resultados conforman la base para la siguiente fase del proyecto, que contempla la creación de *dashboards* interactivos en Apache Superset, que integrarán y mostrarán los resultados de los años 2012 a 2021 junto con los datos más recientes.

4. CONCLUSIONES

El proyecto "Migración de datos de Moodle a Superset" permitió consolidar una fuente de datos homogénea en PostgreSQL, diseñada específicamente para su uso analítico dentro de Apache Superset, lo que constituye el principal logro técnico del trabajo desarrollado entre septiembre y diciembre de 2024. Este proceso garantizó la integración de los datos del TICómetro correspondientes a los años 2012

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 15C - 15

a 2021, homologando estructuras provenientes de distintas versiones de Moodle en un modelo de datos unificado, confiable y reutilizable para análisis posteriores.

A partir de las migraciones previas en las que se procesaron los datos de los años 2022 a 2024, el alcance del presente reporte se concentró en la migración histórica de los periodos no integrados, bajo criterios de unicidad y consistencia, lo que permitió así completar el acervo digital del TICómetro.

La migración realizada contribuye de manera directa a facilitar la generación de informes técnicos y académicos, al disponer de una fuente de datos estandarizada y verificable que puede ser consultada por diferentes herramientas analíticas, entre ellas Apache Superset. Si bien la generación de gráficas y tableros no forma parte del alcance de este reporte técnico, la estructura creada constituye la base fundamental sobre la cual podrán desarrollarse posteriormente los *dashboards* interactivos previstos para el trabajo complementario que dará continuidad al proyecto.

Asimismo, el proceso dio como resultado dos productos adicionales: en primer lugar, los archivos en formato Excel, que consolidan los datos migrados y permiten la consulta, validación y análisis inmediato por parte de investigadores, docentes, funcionarios universitarios y público en general interesado en los niveles de competencia digital de los estudiantes de la UNAM; en segundo lugar, los *scripts* en Python ejecutados en Google Colaboratory Notebooks, que documentan paso a paso la extracción, transformación y carga de los datos. Ambos productos, junto con los esquemas por año creados en la base de datos final en PostgreSQL, constituyen la documentación detallada del proceso de migración y permiten su réplica o actualización en futuras versiones del sistema.

En conjunto, este trabajo técnico representa un avance sustancial en la infraestructura analítica del TICómetro, al ofrecer un entorno unificado para el manejo de datos históricos y recientes, lo que promueve la transparencia, la interoperabilidad y la continuidad institucional que ha caracterizado a los proyectos de evaluación de habilidades TIC en la UNAM desde sus inicios.

AGRADECIMIENTOS

El autor expresa su agradecimiento a la DGTIC de la UNAM por el apoyo institucional brindado para la realización del proyecto “Migración de datos de Moodle a Superset”, desarrollado entre septiembre y diciembre de 2024, en especial a Angélica Ramírez Bedolla.

En particular, se reconoce la valiosa colaboración de Javier Rodrigo Díaz Espinosa por proporcionar los *scripts* y la máquina virtual utilizados como referencia en las migraciones previas, así como a Miguel Zúñiga González por el respaldo y acceso a los servidores que permitieron realizar las extracciones de datos históricos.

Asimismo, se agradece la participación de Cristian Ricardo Ortega Ramírez, responsable del diseño del modelo de datos de Superset y del esquema de conexión utilizado en la visualización de resultados, así como el apoyo de José Larios Delgado y de César Ordóñez Rodríguez en la transferencia de conocimientos sobre la interfaz de creación de tableros del TICómetro con la herramienta de Superset, ya que sin su apoyo y asesoría no habría sido posible la puesta en línea de la información durante el año 2025.

Finalmente y de manera muy especial, se reconoce la colaboración de Néstor Abdy García Fragoso, cuyo apoyo en la programación en Python y en el uso de la herramienta Google Colaboratory (Colab)

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.113 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 15D - 15

fue determinante para la elaboración y depuración de los *scripts* de migración; su asesoría técnica hizo posible completar satisfactoriamente el proceso.

REFERENCIAS

Apache Superset. (2024). *Apache Superset™ es una plataforma moderna de exploración y visualización de datos de código abierto*. https://superset.apache.org/

Devi, K. S., & Aparna, M. (2020). Moodle–An effective learning management system for 21st century learners. *Alochana Chakra Journal,* 9(6), 4474-4485. https://www.researchgate.net/profile/Kuruva-Devi/publication/342259946_Moodle_-An_Effective_Learning_Management_System_for_21_st_Century_Learners/links/5eeafbf492851ce9e7ec87a5/Moodle-An-Effective-Learning-Management-System-for-21-st-Century-Learners.pdf

Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). (2012). *TICómetro: Instrumento para la autoevaluación de habilidades digitales*. Universidad Nacional Autónoma de México. https://educatic.unam.mx/publicaciones/ticometro/TICometro2012.pdf.

Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). (2025). *TICómetro para la evaluación de habilidades digitales*. Universidad Nacional Autónoma de México. https://educatic.unam.mx/servicios/ticometro.html

Moodle (2025) *Dónde empezó todo: La historia de Moodle*. https://moodle.com/es/acerca-de/la-historia-de-moodle/

Sanz, R. (2023). Big Data y OLAP con Superset (Airbnb). TodoBI. https://todobi.com/big-data-olap-con-superset-airbnb/

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 16 - 33

Diseño e implementación de infraestructura tecnológica para la Clínica de Salud Visual

Información del reporte:

Para citar este reporte técnico:

Galicia Espinosa et al. (2025). Diseño e implementación de infraestructura tecnológica para la Clínica de Salud Visual. *Cuadernos Técnicos Universitarios de la DGTIC, 3* (3) páginas(16 - 33).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114

Erika Galicia Espinosa
Escuela Nacional de Estudios Superiores, Unidad León
Universidad Nacional Autónoma de México
egaliciae@enes.unam.mx
ORCID: 0009-0001-6937-0080

Laura Leticia García Sánchez
Escuela Nacional de Estudios Superiores, Unidad León
Universidad Nacional Autónoma de México
lgarcias@enes.unam.mx
ORCID: 0009-0007-3058-5758

Luis Fernando Hernández Zimbrón
Escuela Nacional de Estudios Superiores, Unidad León
Universidad Nacional Autónoma de México
lhernandez@enes.unam.mx
ORCID: 0000-0002-5098-367X

Resumen

La Escuela Nacional de Estudios Superiores, Unidad León de la Universidad Nacional Autónoma de México, construyó e implementó la infraestructura tecnológica especializada en la Clínica de Optometría Salud Visual, con el fin de fortalecer la formación clínica del alumnado y brindar servicios diagnósticos de alta calidad. Se realizó un levantamiento de la infraestructura tecnológica existente para garantizar la compatibilidad de nuevos equipos con las redes de telecomunicaciones, cableado estructurado, fibra óptica y Circuito Cerrado de Televisión. Dado lo anterior, la implementación incluyó diseño e instalación de sistemas modulares de categoría 6A, integración de Access Points (AP por sus siglas en inglés), configuración

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 17 - 33

de VLANs, telefonía IP y conectividad de equipos especializados como el Humphrey Field Analyzer 3. La metodología del proyecto se basó en el enfoque PMBOK, con etapas de diseño, planificación, ejecución y cierre. Los resultados mostraron un funcionamiento estable de los servicios tecnológicos y validación de la infraestructura por parte del personal responsable. Se concluyó que la integración tecnológica incrementa la eficiencia del servicio clínico y fortalece la práctica educativa, con posibilidad de replicabilidad en otras unidades académicas.

Palabras clave:

Infraestructura tecnológica, redes, cableado estructurado, servicios tecnológicos, PMBOK.

Abstract

The National School of Higher Studies, León Unit of the National Autonomous University of Mexico, built and implemented specialized technological infrastructure at the Optometry and Visual Health Clinic to strengthen the clinical training of students and provide high-quality diagnostic services. A survey of the existing technological infrastructure was conducted to ensure the compatibility of new equipment with telecommunications networks, structured cabling, fiber optics, and closed-circuit television. Given this, the implementation included the design and installation of Category 6A modular systems, integration of Access Points (APs), VLAN configuration, IP telephony, and connectivity for specialized equipment such as the Humphrey Field Analyzer 3. The project methodology was based on the PMBOK approach, with stages of design, planning, execution, and closure. The results showed stable operation of the technological services and validation of the infrastructure by the responsible staff. It was concluded that technological integration increases the efficiency of clinical services and strengthens educational practice, with the possibility of replicability in other academic units.

Keywords:

Technological infrastructure, networks, structured cabling, technological services, PMBOK.

1. INTRODUCCIÓN

La salud visual es un componente fundamental para el bienestar de la población y para el desempeño académico del alumnado. En las últimas décadas, los avances tecnológicos aplicados a la optometría han transformado el diagnóstico y la atención clínica al permitir procedimientos más precisos, eficientes y personalizados. Estos avances incluyen la incorporación de equipos de imagenología avanzada, como la tomografía de coherencia óptica (OCT), retinógrafos digitales, dispositivos para evaluar el campo visual, entre otros, los cuales requieren infraestructuras de telecomunicaciones robustas, seguras y adaptables para operar correctamente.

La creciente dependencia de servicios tecnológicos en entornos clínicos, educativos y de investigación hace indispensable planificar, instalar y validar redes de voz, datos y video bajo estándares de calidad y normativas institucionales. De acuerdo con la Dirección General de Cómputo y Tecnologías de Información y Comunicación (DGTIC, 2017), los espacios universitarios deben contar con infraestructura de conectividad que garantice la continuidad de las operaciones clínicas y académicas, así como la seguridad de la información.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 18 - 33

En este contexto, la Escuela Nacional de Estudios Superiores (ENES), Unidad León de la Universidad Nacional Autónoma de México (UNAM), incorporó, en 2017, la licenciatura en Optometría, la cual requiere espacios clínicos con equipamiento de vanguardia para la formación práctica del alumnado y la prestación de servicios especializados a la comunidad. Para atender esta necesidad, se aprobó la construcción de la Clínica de Optometría Salud Visual (CSV), inaugurada en agosto de 2023, cuyo diseño y operación representó retos técnicos significativos relacionados con la compatibilidad de la infraestructura tecnológica existente, la escalabilidad de los sistemas y el cumplimiento de estándares técnicos y normativos.

La planeación estratégica y la ejecución de la infraestructura de las Tecnologías de la Información y la Comunicación (TIC) para la CSV contemplaron la integración de servicios de telefonía IP, datos, Circuito Cerrado de Televisión (CCTV) y redes inalámbricas, todo ello coordinado por personal especializado en tecnologías de la información y comunicación, en colaboración con diversas instancias institucionales.

Este reporte técnico tiene como objetivo documentar de forma detallada la planeación, instalación y validación de la infraestructura tecnológica especializada de la Clínica de Optometría Salud Visual de la ENES León, UNAM, como parte de la calidad de los servicios educativos y clínicos que requiere la licenciatura en Optometría.

2. DESARROLLO TÉCNICO

La optometría, definida por Monroe J. Hirsch y Ralph E. Wick (1968) como "El arte y la ciencia del cuidado de la visión", ha evolucionado desde una práctica enfocada a la venta de anteojos hacia una disciplina científica integral, centrada tanto en el diagnóstico, tratamiento y prevención de problemas visuales como en la promoción de la salud visual (Bromberg, 2009). Actualmente, las y los optometristas desempeñan un rol clave en la atención primaria de la salud visual, así como en la detección temprana de enfermedades oculares con un enfoque holístico y basado en la evidencia científica.

Esta evolución no sólo ha beneficiado la práctica clínica, sino que también ha puesto de manifiesto la relevancia de la salud visual en otros ámbitos, como el educativo. La salud visual es esencial para el rendimiento académico del alumnado, ya que las deficiencias visuales pueden afectar negativamente su capacidad de aprendizaje y concentración (Collins et al., 2017). De igual manera, es importante para la población general que requiere atención en salud visual (Collins et al., 2017; Maples, 2003). Así, la optometría se consolida como un pilar no sólo en la salud, sino también en el desarrollo integral del alumnado.

Esta disciplina se ha modernizado significativamente y ahora cuenta con equipos de tecnología de frontera para el diagnóstico y manejo de diversas patologías oculares. Por ejemplo, se emplean dispositivos avanzados para la detección temprana de condiciones como la retinopatía diabética y el glaucoma, permitiendo intervenciones más eficaces. Existen también salas 3D en las que se recrean ambientes y entornos cotidianos tridimensionales para terapia visual. Por otra parte, los equipos de tomografía de coherencia óptica (OCT) y topografía corneal permiten un análisis detallado de la retina y la superficie ocular, facilitando diagnósticos precisos y personalizados.

En dicho contexto de innovación tecnológica, la optometría cobra especial relevancia frente a los desafíos de ofrecer servicios de atención visual de calidad y con tecnología de punta a la población de la región

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 19 - 33

del Bajío. Por ello, la planificación de la infraestructura tecnológica y equipamiento especializado de la Clínica de Optometría Salud Visual (CSV) inició en febrero del 2021; en este proceso, participaron personal de la Clínica, el Departamento de Cómputo e Informática, la Superintendencia de Obras de la ENES León, la Dirección de Telecomunicaciones de la DGTIC y la Dirección General de Obras y Conservación (DGOC) de la UNAM. Gracias a la coordinación y colaboración de estas áreas, se logró diseñar e implementar un espacio equipado con tecnología actual y recursos óptimos para la atención visual; tras meses de trabajo en conjunto, el 19 de agosto de 2023 se inauguró la clínica.

Los diferentes ambientes y espacios de la CSV están cuidadosamente diseñados para fomentar la formación del alumnado y brindar atención integral de alta calidad a los pacientes. Sin embargo, el funcionamiento adecuado de los modernos consultorios de optometría no sería posible sin una infraestructura de telecomunicaciones eficaz.

Como parte de la etapa de diseño, se decidió que los nuevos servicios se integraran a la infraestructura ya existente con la finalidad de gestionar todos los recursos tecnológicos de manera centralizada. Esto simplifica mantenimientos y reduce costos, ya que optar por una nueva tecnología podría implicar inconsistencias en la calidad del servicio, además de contemplar e incorporar más equipos, servidores y controladoras, así como la gestión de administración y mantenimientos independientes.

Asimismo, entre las principales ventajas de implementar tecnología compatible a la existente, se encuentra la de eficientar recursos y reducir los riesgos de implementación, ya que se cuentan con configuraciones validadas y con los servicios funcionando adecuadamente en la institución.

La planeación de la infraestructura tecnológica de la Clínica de Optometría implicó tomar decisiones estratégicas sobre la elección de componentes de red, cableado estructurado, equipos especializados y su integración. Para garantizar la estabilidad, escalabilidad y compatibilidad del sistema, se realizó un análisis comparativo entre distintas soluciones. Se evaluaron diferentes categorías y marcas de cableado estructurado, optando por la categoría 6A de la marca Panduit por su confiabilidad, compatibilidad con la infraestructura institucional existente, además de ser uno de los cableados con velocidad de transmisión alta y garantía de 25 años. En cuanto a la red inalámbrica, se seleccionó la solución Cisco Meraki por su capacidad de integración con la infraestructura instalada, facilidad de gestión y licenciamiento institucional compatible. Estas decisiones técnicas fueron tomadas en conjunto con especialistas en TIC de la ENES León, en coordinación con el personal de la Clínica y de la DGOC, con el fin de lograr una solución robusta, segura y replicable.

En este sentido, la experiencia documentada es replicable, ya que presenta una metodología clara, decisiones justificadas y una validación funcional del sistema implementado, lo que permite orientar a otras unidades académicas en proyectos similares. Además, se integraron estándares internacionales como las disposiciones en materia de instalaciones de telecomunicaciones UNAM, fortaleciendo así la base técnica de cada decisión adoptada, que además contemplan e integran la norma internacional ISO/IEC 11801 (Disposiciones en materia de instalaciones de telecomunicaciones, 2017).

Infraestructura especializada de la Clínica de Optometría

Como parte de la planificación, se consideran tres áreas destinadas a equipos especiales, los cuales son:

- Tomógrafo de Coherencia Óptica (OCT): Sánchez Ruiz (2020) describe al OCT como un equipo de imagen no invasiva y de alta resolución que permite visualizar en detalle las estructuras internas del ojo, especialmente las capas de la retina y el nervio óptico. A través de ondas de luz, el OCT

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 20 - 33

genera imágenes transversales que muestran cortes precisos de los tejidos oculares, permitiendo el análisis detallado de su morfología y grosor. La funcionalidad del OCT es crucial en el diagnóstico y seguimiento de diversas patologías oculares. Su uso en la clínica brinda al alumnado la oportunidad de especializarse en diagnóstico clínico mediante tecnología avanzada.

- Cámara de fondo de ojo (retinografía): Orlando (2017) define que este equipo permite capturar imágenes detalladas de la retina, el nervio óptico y los vasos sanguíneos en el interior del ojo. Es una técnica no invasiva que se utiliza para detectar patologías oculares como la retinopatía diabética, glaucoma y la degeneración macular, que se han identificado como las principales causas mundiales de ceguera prevenible. Su uso en la clínica brinda al alumnado una comprensión práctica sobre la importancia del diagnóstico temprano y la prevención en el campo de la salud visual.
- Equipo para evaluar Sensibilidad al Contraste (SC): Tripolone (2018) identifica que es una herramienta útil para la caracterización de la visión espacial del sistema visual humano. Para el alumnado, manejar y contar con este equipo significa tener la oportunidad de comprender una dimensión más profunda de la evaluación visual, más allá de las pruebas de sensibilidad rutinarias. Cabe mencionar que es único en Latinoamérica.
- Campímetro (campos visuales): Valle (2020) menciona que la campimetría visual es una prueba oftalmológica que se realiza para valorar el campo visual de una persona. Su realización es de gran importancia para detectar patologías que producen pérdidas en dicho campo visual, algunas de ellas irreversibles. Este equipo permite a los estudiantes experimentar con una herramienta clave para detectar y monitorizar afecciones que impactan la visión periférica, lo cual es fundamental para evaluar el estado funcional del campo visual en los pacientes.

La planeación del proyecto incluyó un análisis funcional y operativo de los equipos clínicos de alta especialidad, como el Humphrey Field Analyzer 3 (HFA3), el OCT y los retinógrafos digitales. Estas tecnologías requieren condiciones específicas de conectividad y suministro eléctrico. En el caso del HFA3, se verificó que la toma de corriente fuera regulada, con línea de tierra dedicada y protección contra variaciones de voltaje, conforme a las recomendaciones del fabricante.

A nivel informático, se asignaron direcciones IP fijas, integración mediante *switches* y segmentación de red mediante VLANs, garantizando la estabilidad de la transmisión y seguridad de los datos. Los equipos se ubicaron en función de criterios clínicos y ergonómicos validados por el área usuaria, y sus requerimientos se incorporaron desde la fase de diseño del edificio y del cableado estructurado.

Como parte de las consideraciones técnicas, fue necesaria la adquisición de impresoras compatibles con el lenguaje Adobe Postcript 3, el cual utiliza superceldas que multiplican por cuatro la cantidad de niveles de gris que se pueden imprimir. Esta tecnología también ayuda a los dispositivos de alta resolución, como las fotocomponedoras, a imprimir 4096 tonos de gris en cada colorante para producir imágenes con mezclas más suaves.

En el caso de la instalación de impresoras en el equipo Humphrey Field Analyzer 3, la modificación de configuración se realizó tras identificar que la opción predeterminada del sistema no permitía la integración de impresoras convencionales. Se optó por ingresar al modo de servicio del equipo para realizar el ajuste y evitar así la instalación de *drivers* externos que pudieran afectar la estabilidad del software.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 21 - 33

Esta decisión se tomó tras analizar las recomendaciones técnicas del fabricante del HFA3 y las restricciones del sistema operativo embebido. Asimismo, se consultó al personal clínico responsable del uso del equipo, quienes confirmaron que, tras el cambio, el funcionamiento fue adecuado y no se presentó ninguna afectación al desempeño del sistema. No fue necesaria la intervención del proveedor, ni se realizaron modificaciones que comprometieran la garantía del equipo, ya que el ajuste se realizó dentro de las opciones de configuración autorizadas por el fabricante.

La infraestructura tecnológica implementada fue diseñada específicamente para satisfacer las necesidades clínicas de la licenciatura en Optometría. Los espacios físicos y lógicos permiten que los estudiantes se capaciten con equipos clínicos reales, replicando escenarios profesionales. En el desarrollo técnico, se priorizó la integración de tecnologías que facilitaran el diagnóstico visual, el análisis de imágenes y la conectividad entre áreas clínicas, administrativas y académicas. Por ello, cada decisión técnica en la infraestructura responde a requerimientos del modelo educativo clínico.

Infraestructura tecnológica

El edificio de la Clínica de Optometría se conforma de dos niveles, donde, en cada uno, se instalaron y se realizaron adecuaciones al cuarto de telecomunicaciones; estos espacios están dedicados a la organización, gestión de cables y equipos de telecomunicaciones.

Además, y como parte de la infraestructura tecnológica, se suministraron, instalaron y configuraron los dispositivos de telecomunicaciones necesarios para brindar servicios de VoIP, datos, CCTV y WiFi a la nueva Clínica de Optometría.

Equipamiento

El equipamiento de *switches* se definió con base en la compatibilidad de la tecnología ya instalada en la institución, considerando la velocidad, tipos y cantidad de puertos, así como las funcionalidades avanzadas para los servicios ofrecidos como PoE, para alimentar las cámaras de CCTV, y que fueran gestionables, con el fin de segmentar la red por medio de *Virtual Local Area Network* (VLAN, por sus siglas en inglés)

Además, para garantizar la continuidad del suministro eléctrico, incrementar la vida útil de los equipos y brindar protección a los equipos de telecomunicaciones, se instaló un Sistema de Alimentación Ininterrumpida (UPS por sus siglas en inglés) y un aire acondicionado en cada cuarto de telecomunicación del nuevo edificio de Optometría.

Cableado

En la actualidad, la conexión por fibra óptica se ha consolidado como la infraestructura fundamental para la conectividad. Por lo tanto, para conectar el cuarto principal de telecomunicaciones (CP) con el cuarto de telecomunicaciones (CT) del edificio de la Clínica de Optometría, como se muestra en la Figura 1, fue necesario trazar la trayectoria, realizar la obra, canalización y cableado de fibra óptica, además de verificar la disponibilidad de puertos en el dispositivo de red principal, el cual distribuye la conectividad y el tráfico de datos de la red de la ENES Unidad León.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 22 - 33

Figura 1

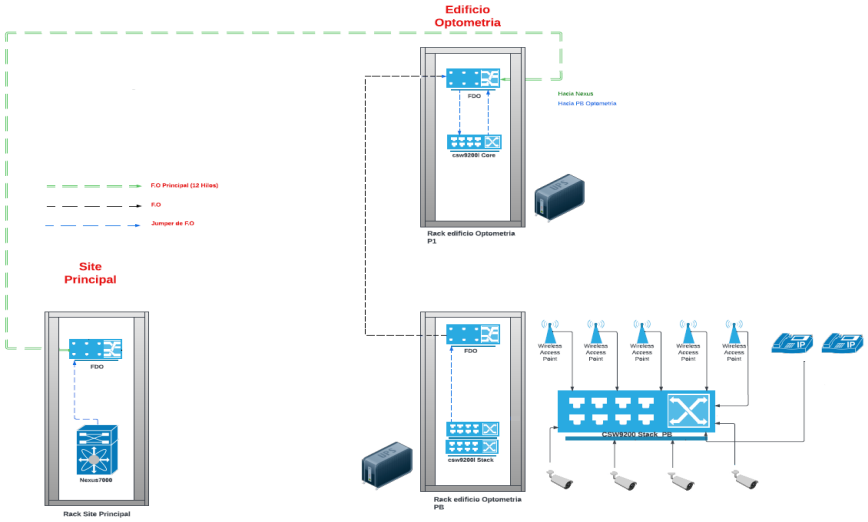
Distribuidor de fibra óptica

Es importante mencionar que se tomó como base el proyecto original de la institución, ya que se encuentra funcionando en una topología de estrella, la cual lleva cada servicio punta a punta desde el CP hasta los cuartos de telecomunicación de los diferentes edificios de la ENES León.

La instalación de fibra óptica, como se puede apreciar en la Figura 2, se basó en el sistema de topología existente, saliendo un enlace de fibra óptica de 6 hilos multimodo 50/125 µm OM3 del CP al CT de la clínica, ubicado en el segundo nivel.

Figura 2

Integración de la fibra óptica



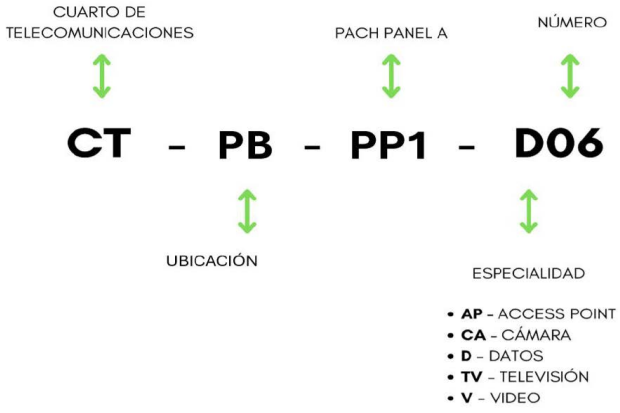
https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 23 - 33

En la instalación del sistema de cableado estructurado de la clínica, se implementó un sistema modular categoría 6A marca Panduit, contemplando nodos de VoIP, datos, CCTV y nodos para AP distribuidos de forma estratégica en los dos niveles del edificio de la clínica, llevando un recorrido hacia el cuarto de telecomunicaciones correspondiente, con un desplazamiento con canalización por muros, piso y plafón.

Con la finalidad de organizar y diferenciar visualmente las conexiones en los cuartos de telecomunicaciones, los cables de parcheo (*patch cord*) se catalogaron por colores: los negros se se asignaron a la conexión de los AP, los blancos al sistema de videovigilancia (CCTV) y los azules a Voz/Datos. Asimismo, se implementó una nomenclatura uniforme para todos los nodos, como se muestra en la Figura 3, lo que contribuye a mejorar la eficiencia, la seguridad y la facilidad de mantenimiento dentro de la infraestructura de cableado estructurado.

Figura 3

Listado de nomenclatura utilizado en el cuarto de telecomunicaciones (CT), planta baja (PB), panel (PP1), número de servicio (D06)



Es importante mencionar que, para la infraestructura de cableado estructurado, se realizó la Certificación Panduit con garantía del sistema por 25 años.

VoIP

Con relación a la telefonía, se integraron equipos telefónicos IP de la marca Cisco, instalados y distribuidos de manera estratégica dentro de la Clínica, con la finalidad de optimizar la comunicación tanto interna como externa. Además, se integraron las mismas funcionalidades de la telefonía actual, por ejemplo, la marcación rápida, el desvío de llamadas y la posibilidad de realizar conferencias telefónicas.

Circuito Cerrado de Televisión (CCTV)

Actualmente, la implementación de un sistema del CCTV es fundamental para prevenir incidentes y para el cuidado de las instalaciones, por lo que, para el nuevo edificio de la Clínica, se consideraron cámaras tipo domo, panorámicas y tipo bala, de la marca HikVision, con la finalidad de integrarlos en el *Network Video Recorder* (NVR por sus siglas en inglés) funcionando actualmente. La ubicación e instalación de cada tipo de cámara se sustentó con base en las características específicas, el espacio, así como el propósito de vigilancia de cada área de la clínica.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 24 - 33

Red inalámbrica

Para contar con cobertura inalámbrica dentro del edificio, se suministraron e instalaron los AP (ver Figura 4), mismos que fueron estratégicamente distribuidos para maximizar la conectividad en todas las áreas de la clínica. Estos dispositivos permiten establecer una red inalámbrica y facilitan la movilidad, acceso a Internet y recursos de red.

Figura 4

Access Point (AP) instalado

2.1 METODOLOGÍA

La gestión del proyecto se basó en el enfoque del Project Management Institute (PMI), utilizando como referencia la guía PMBOK®(Project Management Institute, 2021). Este estándar proporciona una estructura metodológica para la planificación, ejecución, monitoreo y cierre de proyectos complejos, y ha sido ampliamente adoptado en proyectos de tecnologías de la información. Se eligió este modelo por su capacidad para organizar las actividades de forma secuencial, establecer responsabilidades claras, gestionar riesgos y asegurar el cumplimiento de los objetivos en entornos institucionales. Las etapas del proyecto incluyeron diseño, configuración, instalación y pruebas, lo que permitió controlar de forma eficiente los diferentes procesos técnicos involucrados en la puesta en marcha de la infraestructura tecnológica de la Clínica de Optometría.

2.1.1 INICIO

Dentro de esta fase, se llevaron actividades, en conjunto con la Superintendencia de Obras de la ENES León, para realizar los planos de la infraestructura de red, comunicaciones y seguridad, con la finalidad de analizar y evaluar los espacios, ubicar los nodos de red de voz y datos, considerando las necesidades de los usuarios, así como el equipamiento de CCTV, equipos de cómputo, telefonía y equipo especializado.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 25 - 33

En la primera etapa, se consideró el equipamiento para la creación de veinte consultorios; uno de ellos se destinó a la investigación, dos más para optometría pediátrica y uno de consulta para lentes de contacto. También se planificó la implementación de las áreas de óptica y profundización.

2.1.2 PLANIFICACIÓN

A través de la colaboración con personal de la Dirección de Telecomunicaciones de la DGTIC, se realizó la revisión de los requerimientos para el desarrollo del proyecto, con relación a la cantidad de nodos (Voz/Datos, CCTV y AP) que debían contemplarse en las distintas áreas del edificio. Del mismo modo, se realizaron planos, estudios de cobertura con software de simulación para la red inalámbrica local y se brindaron recomendaciones para promover buenas prácticas en el desarrollo del proyecto.

Como parte de la planificación del cableado estructurado, se analizó la infraestructura física existente, la ruta del cableado más adecuado, los equipos (marcas / modelos) en funcionamiento, la distribución correcta de los nodos y la distancia entre los puntos de conexión.

Como parte de las consideraciones para el despliegue de la red inalámbrica, se consideró la tecnología ya instalada en la institución. Lo anterior, con la finalidad de asegurar la compatibilidad y eficiencia en la integración de los nuevos dispositivos. Por ejemplo, la marca y modelos de los AP, la integración a la controladora (*dashboard*) y el licenciamiento necesario. Además, se planificó la distribución de los AP considerando factores como el tamaño de los espacios, la cantidad de usuarios a conectarse y la necesidad de minimizar interferencias, lo que permitiría ofrecer una experiencia de conexión fluida y confiable que apoye al profesorado, alumnado y pacientes.

Para la planificación del CCTV, se realizó una revisión detallada de las marcas y modelos de las cámaras instaladas previamente en la ENES, así como de la capacidad del NVR, siendo este dispositivo el responsable de almacenar y gestionar el video capturado por las cámaras de seguridad IP. Este análisis fue crucial para garantizar que el NVR pudiera soportar la cantidad de cámaras, almacenamiento y resolución de video configurada, asegurando así un funcionamiento óptimo del sistema.

Además del sistema CCTV, se abordó la infraestructura de telefonía, considerando equipos IP compatibles con el *Cisco Unified Communications Manager* (CUCM por sus siglas en inglés) que es la plataforma que permite gestionar y controlar las llamadas dentro de la red de la universidad, lo que permite asegurar la integración y operatividad del sistema telefónico con el resto de la infraestructura tecnológica.

2.1.3 EJECUCIÓN

Una vez realizado el cableado y las pruebas de transmisión de datos, se procedió con la instalación y configuración de los *switches* suministrados. Para esto, se analizó la segmentación existente en la institución, la cual, por motivos de seguridad, está organizada mediante VLAN. Este enfoque permite aislar diferentes tipos de tráfico, mejorar la seguridad y garantizar un acceso controlado. Asimismo, se configuró cada puerto del *switch* asignándole la VLAN correspondiente a su servicio CCTV, VoIP, datos y AP (ver Figura 5).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 26 - 33

Figura 5

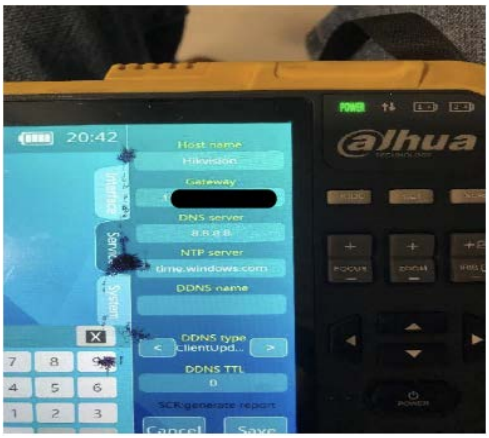
Configuración de VLAN en switches

```
<<Enlace F.O P1_MD connected    trunk       full    10G SFP-10GBase-SR
<<AP_PB>>          connected    25        a-full a-1000 10/100/1000BaseTX
<<AP_PB>>          connected    25        a-full a-1000 10/100/1000BaseTX
<<AP_PB>>          connected    25        a-full a-1000 10/100/1000BaseTX
<<AP_PB>>          connected    25        a-full a-1000 10/100/1000BaseTX
<<AP_PB>>          connected    25        a-full a-1000 10/100/1000BaseTX
<<ptos_CCTV>>      connected    67        a-full  a-100 10/100/1000BaseTX
<<ptos_CCTV>>      connected    67        a-full a-1000 10/100/1000BaseTX
<<ptos_CCTV>>      connected    67        a-full  a-100 10/100/1000BaseTX
<<ptos_CCTV>>      connected    67        a-full  a-100 10/100/1000BaseTX
<<ptos_CCTV>>      connected    67        a-full a-1000 10/100/1000BaseTX
```

Para las cámaras de seguridad IP instaladas en el edificio de Optometría, se asignó una VLAN específica y se realizó una configuración detallada de cada dispositivo. A cada cámara, se le asignó una dirección IP única, y se configuró el *gateway* correspondiente para garantizar su correcta integración a la red (ver Figura 6). Además, se configuró el *Network Time Protocol* (NTP por sus siglas en inglés) en cada cámara para sincronizar la hora de forma precisa y asegurar así la uniformidad en los registros de video.

Figura 6

Validación de cámara IP

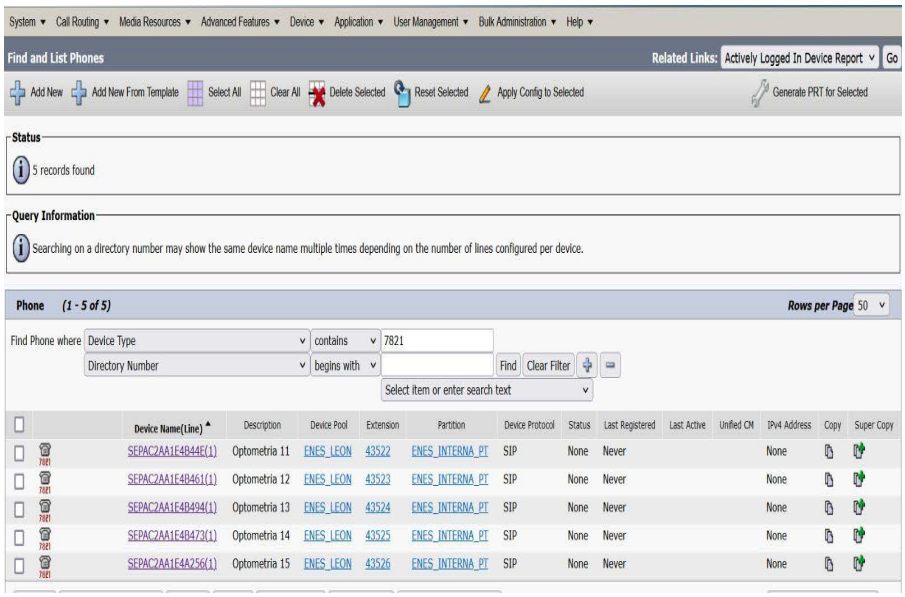


Una vez configurados los puertos de los *switches*, se procedió a integrar el sistema de telefonía (ver Figura 7). Lo anterior requirió la configuración de la salida a Internet y la incorporación de los DNS correspondientes en la tarjeta de red del servidor CUCM. Este paso fue fundamental para localizar los servidores del fabricante y llevar a cabo la validación requerida. La activación permitió gestionar el servidor de telefonía durante un período de 90 días, tiempo en el cual se realizaron las configuraciones necesarias, dado que actualmente no se cuenta con el licenciamiento requerido para la incorporación de nuevos dispositivos.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 27 - 33

Figura 7

Integración de la telefonía en el CUCM



Asimismo, se instalaron los AP en la planta baja del edificio, lo que permitió establecer una red inalámbrica para el profesorado, alumnado, personal administrativo y pacientes de la clínica. Los dispositivos fueron integrados en la red existente a través del *dashboard*, configurándose con los *Service Set Identifier* (SSID, por sus siglas en inglés) y las políticas de seguridad previamente definidas y funcionales de la ENES León. Es importante mencionar que estos equipos pueden alcanzar velocidades de 1 Gbps (1000 Mbit) y configuraciones de dúplex completo como se muestra en la Figura 8, lo que permite que el dispositivo pueda enviar y recibir datos simultáneamente a través del puerto. Además, en la Figura 9, se muestra una métrica que ayuda a monitorear el tráfico de datos de uno de los dispositivos.

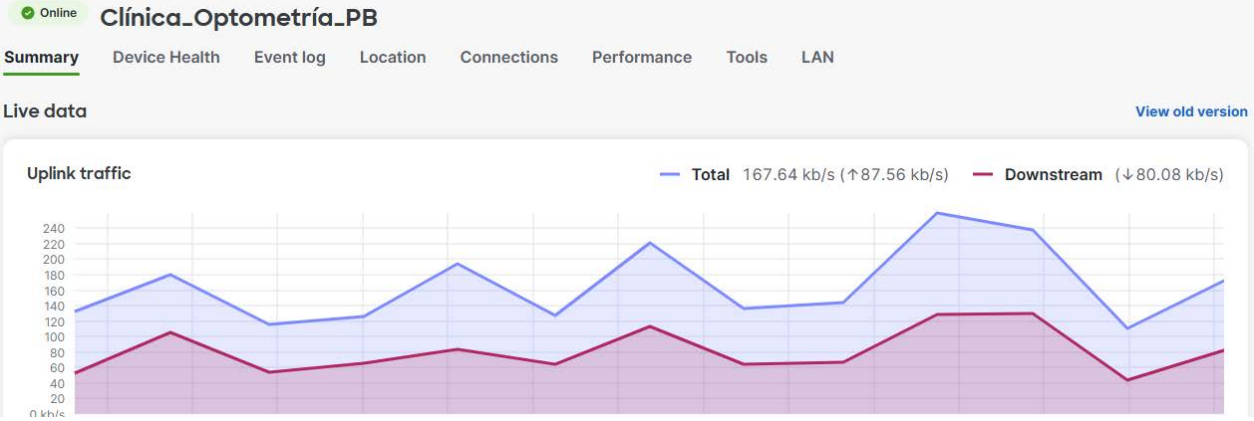
Figura 8

Integración de los Access Point (AP) al dashboard

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 28 - 33

Figura 9

Uplink Traffic de un Access Point (AP)



Como parte del seguimiento, se verificaron los avances referentes a la construcción y equipamiento del edificio de Optometría mediante minutas, validaciones y recorridos en sitio; queda pendiente la finalización de la obra del segundo nivel, así como la instalación de la infraestructura de red inalámbrica y la telefonía IP. Actualmente se realizan las gestiones correspondientes para que los trabajos de instalaciones se lleven a cabo de manera correcta y completa, garantizando que el nuevo espacio cumpla con las características requeridas para ofrecer una atención clínica y educación de alta calidad.

La validación de los servicios del Circuito Cerrado de Televisión, se realizó midiendo la conectividad y respuesta por medio de la interfaz de línea de comandos, ejecutando “ping”, que es la utilidad de diagnóstico para medir la latencia de respuesta y conexión, lo cual indica si la cámara se encuentra en línea y disponible, además de medir la correcta conectividad al NVR. Del mismo modo, se verificó la visualización en tiempo real, la grabación y reproducción de video.

En los servicios de la telefonía IP, se corroboró la correcta configuración e integración al CUCM de los dispositivos, la conectividad entre extensiones y la capacidad de recibir llamadas tanto internas como externas, mediante la interfaz gráfica (ver Figura 7).

Referente a los servicios de red inalámbrica, se validó la cobertura, la intensidad de la señal, la integración al *dashboard* y el licenciamiento adecuado de los nuevos dispositivos. Además, se verificó la velocidad en los diferentes SSID que funcionan en la institución, como son: red RIU, eduroam, PC Puma ENES León y PC Puma Académicos.

Para la red alámbrica, se revisó cada nodo de red, la velocidad tanto de carga como de descarga y la correcta configuración de VLAN en el switch.

Finalmente, para realizar las pruebas o validaciones de los servicios tecnológicos, se utilizaron herramientas y plataformas especializadas que permiten evaluar tanto la instalación física como el correcto funcionamiento y desempeño de cada servicio, además de utilizar el protocolo TCP/IP como base para la transmisión de datos entre los diferentes dispositivos.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 29 - 33

2.1.4 CIERRE

La empresa líder en productos y servicios de infraestructura para redes de datos y aplicaciones de energía eléctrica, Panduit, emitió el certificado de garantía de cableado estructurado, asegurando el cumplimiento de la norma EIA-TIA 568-B (*Electronic Industry Association* y *Telecommunication Industry Association*), véase Anexo A Certificación del cableado estructurado.

La funcionalidad de los equipos instalados, incluyendo los especializados, fue validada por el personal responsable de la CSV, quienes realizaron el proceso correspondiente de revisión y pruebas. Este procedimiento garantiza que los pacientes reciban un servicio confiable y efectivo en su atención visual y que el alumnado pueda llevar a cabo su práctica clínica en un ambiente funcional y eficaz

3. RESULTADOS

Los resultados se muestran en correspondencia directa con los objetivos y la metodología aplicada, lo que permite validar el cumplimiento de los procesos técnicos implementados.

La instalación y configuración de la infraestructura especializada se llevó a cabo en conjunto con el personal de soporte técnico de la marca de los equipos especializados que se ilustran en las Figuras 10, 11 y 12, los cuales fueron validados mediante la realización de pruebas por parte del equipo de tecnologías, el profesorado y responsables de la Clínica de Optometría.

A continuación, se presentan imágenes de la implementación de los servicios tecnológicos y digitales necesarios para el buen funcionamiento de la clínica.

Figura 10

Consultorio equipado de la Clínica de Optometría. A la derecha de la imagen, se observa el sillón y a un costado la lámpara de hendidura

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 30 - 33

Figura 11

Equipo especializado Oculus Pentacam

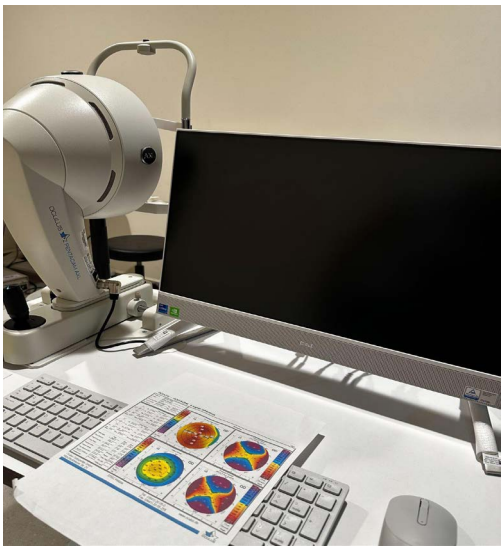


Figura 12

Equipo de retinografía Clarus 500

La infraestructura instalada impacta en la atención visual y formación profesional. En abril de 2024, la licenciatura en Optometría obtuvo la acreditación por un período de cinco años, otorgada por los Comités Interinstitucionales para la Evaluación de la Educación Superior, un organismo dedicado al aseguramiento de la calidad en programas de estudio. El informe final destacó la pertinencia de la licenciatura para atender las necesidades de la región central de México, así como su infraestructura óptima y el equipamiento de vanguardia para la práctica clínica.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 31 - 33

4. CONCLUSIONES

La implementación de la infraestructura tecnológica especializada para la Clínica de Optometría Salud Visual permitió atender las necesidades de conectividad, integración de equipos clínicos y operación de sistemas tanto de videovigilancia como de telefonía IP; se cumplieron los objetivos de diseño y funcionalidad planteados en la etapa de planificación.

El uso del enfoque metodológico PMBOK facilitó la organización del proyecto en fases estructuradas, lo que garantizó una ejecución eficiente, ordenada y alineada a las buenas prácticas institucionales. La solución tecnológica permitió integrar servicios de red de forma escalable, eficiente y con bajo riesgo de interferencias entre servicios clínicos, administrativos y de seguridad.

Se demostró también que, a través de una planificación precisa y la colaboración interdepartamental, es posible habilitar entornos clínicos de alta tecnología en universidades públicas con recursos limitados.

4.1 RECOMENDACIONES

Para la conexión de la fibra óptica del edificio, fue crucial verificar la compatibilidad de los equipos existentes, ya que el dispositivo principal de telecomunicaciones (*Core*), cuenta con más de diez años en operación, por lo que carece de garantía y contrato de soporte de Cisco (*Smartnet*). Por ello, fue necesario realizar una búsqueda del módulo de transceptor óptico adecuado y compatible, capaz de transmitir datos a través de fibra óptica con alta capacidad de transferencia y alcance a largas distancias. En este contexto, se recomienda evaluar de manera regular las características, limitaciones y capacidades de los equipos de telecomunicaciones instalados en las instituciones, con el fin de asegurar una conexión efectiva en proyectos orientados al fortalecimiento o renovación de la infraestructura tecnológica.

Asimismo, se recomienda contar con el licenciamiento vigente y soporte por parte del fabricante que permita contar con todas las funcionalidades adecuadas para el CUCM, lo cual no solamente permite acceder a todas las características del sistema de telefonía, sino que también garantiza la escalabilidad necesaria para integrar nuevos equipos a medida que crecen las necesidades de la institución.

Se recomienda también verificar las características técnicas y físicas de los equipos especializados de gran volumen, con la finalidad de distribuir de manera efectiva los espacios y conexiones necesarias. Asimismo, es necesario evaluar periódicamente la compatibilidad y renovar el licenciamiento de hardware y software, para evitar obsolescencias tecnológicas. Del mismo modo, se recomienda replicar el modelo metodológico de implementación en otras clínicas universitarias, adaptándolo a las necesidades específicas del entorno.

Finalmente, se recomienda establecer un plan de mantenimiento preventivo para asegurar la continuidad operativa de los sistemas instalados.

AGRADECIMIENTOS

A la Dra. Laura Susana Acosta Torres, Directora de la ENES León, a la Dra. Ma. Concepción Arenas Arrocena, Secretaria General, al Mtro. Salvador Andrade Ortiz, Secretario Académico y a la Mtra. Ana Laura Martínez, responsable de la licenciatura en Optometría; al Dr. Javier de la Fuente Hernández, primer Director y Fundador de la ENES León y actual titular de la Unidad de Extensión en San Miguel de Allende, por su

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 32 - 33

impulso para la creación de un espacio educativo innovador para el alumnado y fortalecer la salud visual de la población en la región y en México.

REFERENCIAS

Bromberg, A. (2009). *Historia de la Optometría en México*. CONACULTA. https://www.cultura.gob.mx/turismocultural/destino_mes/guanajuato/informacion_general.html

Collins, M. E., Wolf, B., Guo, X., Shakarchi, A. F., Madden, N. A., Repka, M. X., Friedman, D. S., & Neitzel, A. J. (2021). Effect of a randomized interventional school-based vision program on academic performance of students in grades 3 to 7: A cluster randomized clinical trial. *JAMA Ophthalmology*, 139(10), 1104–1114. https://doi.org/10.1001/jamaophthalmol.2021.3544

Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (2017). *Disposiciones en materia de instalaciones de telecomunicaciones*. Universidad Nacional Autónoma de México.

Hernández, M. (2023) Abre nueva clínica de Optometría Salud Visual - Gaceta UNAM. *Gaceta UNAM*. Recuperado de https://www.gaceta.unam.mx/abre-nueva-clinica-de-optometria-salud-visual/

Hirsch, M. J., & Wick, R. E. (1968). *The Optometric Profession*. Chilton Book Company.

Maples, W. C. (2003). Visual factors that significantly impact academic performance. *OPTOMETRY-ST LOUIS-*, 74(1), 35-49. PMID 12539891.

Orlando, J. I. (2017). *Aprendizaje automático para asistencia al diagnóstico de enfermedades visuales basado en imágenes de fondo de ojo* [Tesis de licenciatura]. Universidad Nacional del Litoral.

Project Management Institute. (2021). *A guide to the project management body of knowledge (PMBOK® guide) – Seventh edition*. Project Management Institute.

Sánchez Ruiz, D., Castilla Céspedes, M.; Ruiz Laza, A. (2020). Utilidad clínica de la tomografía de coherencia óptica (OCT) en el diagnóstico del deterioro cognitivo tipo Alzhéimer. Recuperado de https://ddd.uab.cat/record/241515

Tripolone, M. C., Issolio, L., Silva, B., Filgueira, C. P., Pérez, D., & Barrionuevo, P. (2018). *Sensibilidad al contraste en pacientes con glaucoma temprano: efectos del nivel de iluminación y la excentricidad*. ANALES AFA (pp. 62-66).

Valle Pérez, D. (2020). *Análisis de estrategias para campimetrías y propuestas alternativas basadas en estadística espacial y redes neuronales*. [Tesis de maestría]. Universidad Nacional Autónoma de México.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.114 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 33 - 33

ANEXO A

Certificación del cableado estructurado

PANDUIT™

se honra en extender el presente

Certificado de Garantía de Sistema por 25 años

para la infraestructura de Cableado Estructurado

realizado por el integrador:

SERVICIOS INTEGRALES DE COMUNICACIONES Y PROCESAMIENTO DE DATOS S.A. DE C.V.

en las Instalaciones de la compañía

Escuela Nacional de Estudios Superiores Unidad León, de la Universidad Nacional Autónoma de México

March 17, 2023 ID 850728

Panduit Latinoamérica
Achievement and Excellence
Quality Guaranteed

La presente instalación cumple con las normas y estándares ISO / IEC, EIA / TIA, NMX.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.115 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 34 - 42

Carga dinámica en tiempo real de entornos tridimensionales para galerías virtuales 3D

Información del reporte:

Para citar este reporte técnico:

Cruz Lovera, T. M. (2025). Carga dinámica en tiempo real de entornos tridimensionales para Galerías Virtuales 3D. *Cuadernos Técnicos Universitarios de la DGTIC, 3* (3) páginas (34 - 42).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.115

Tayde Martín Cruz Lovera
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
taydevr@comunidad.unam.mx
ORCID: 0009-0003-9519-8805

Resumen

Se documenta la solución implementada para la carga dinámica en tiempo real de entornos tridimensionales en galerías virtuales 3D, un servicio que permitirá crear exposiciones virtuales de obras digitales bidimensionales y tridimensionales.

Uno de los principales desafíos en el desarrollo de este tipo de sistemas es la optimización del rendimiento, ya que los entornos 3D suelen implicar un alto costo computacional y tiempos de carga prolongados, especialmente en plataformas web donde los recursos del usuario son muy variables. Para abordar este problema, se implementaron estrategias de optimización para mejorar los tiempos de carga. Además, se exploró el uso de almacenamiento estructurado para gestionar datos generados en tiempo de ejecución, lo que facilitó la reconstrucción de las galerías creadas y la transmisión de información entre el interactivo web y el servidor.

Palabras clave:

Unity, WebGL, WebGPU, JSON, gráficos 3D.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.115 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 35 - 42

Abstract

The implemented solution for real-time dynamic loading of three-dimensional environments into 3D virtual galleries is documented. This service will allow the creation of virtual exhibitions of two- and three-dimensional digital artworks.

One of the main challenges in developing this type of system is performance optimization, as 3D environments typically involve high computational costs and long loading times, especially on web platforms where user resources are highly variable. To address this problem, optimization strategies were implemented to improve loading times. Additionally, the use of structured storage was explored to manage data generated at runtime, which facilitated the reconstruction of the created galleries and the transmission of information between the web interactive and the server.

Keywords:

Unity, WebGL, WebGPU, JSON, 3D graphics.

1. INTRODUCCIÓN

En 2022, el Coordinador del Programa de Posgrado en Artes y Diseño de la Universidad Nacional Autónoma de México se acercó a la Dirección General de Cómputo y de Tecnologías de Información y Comunicación con la necesidad de desarrollar una galería virtual para presentar los trabajos de titulación de cuatro estudiantes. Como respuesta, se diseñó un interactivo 3D navegable, que simulaba una galería con cuatro salas y permitía recorrerla en primera persona, interactuando con las obras.

El proyecto Galerías Virtuales 3D surgió de la necesidad de la comunidad universitaria de contar con un servicio gratuito para montar exposiciones digitales personalizadas, tanto de obras bidimensionales (fotografías, dibujos, pinturas y videos) como tridimensionales (esculturas y modelos). Aunque existen algunas soluciones en el mercado, éstas son de pago o tienen limitaciones en sus versiones gratuitas.

Desde el punto de vista de las tecnologías de información y comunicación, se abordó un problema relevante: la necesidad de desarrollar una experiencia tridimensional interactiva, personalizable y fluida en plataformas web, garantizando buen rendimiento incluso en equipos con recursos limitados. Los entornos virtuales en 3D con múltiples modelos, texturas y materiales presentan altos costos computacionales, lo que representa un desafío particular para navegadores web. Friston et al. (2017) señalan que una solución eficaz para la integración de recursos tridimensionales debe permitir la carga modular y la gestión eficiente de activos digitales en tiempo de ejecución, a fin de facilitar entornos interactivos y escalables en motores como Unity.

Para este proyecto, se eligieron tecnologías modernas y ampliamente utilizadas: Unity para la construcción del entorno 3D interactivo, React para la interfaz web, y un servidor construido en Node.js y Express con base de datos en SQLite. Unity destaca por su capacidad de exportación a WebGL, lo que facilita su ejecución en navegadores sin necesidad de instalar software adicional. Además, estudios como el de Zheng et al. (2023) destacan que motores como Unity ofrecen mayores capacidades de interacción y manejo de iluminación y física avanzada, por lo que superan a implementaciones directas en WebGL en términos de complejidad visual y experiencia de usuario.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.115 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 36 - 42

El objetivo de este reporte técnico es documentar la solución técnica implementada para lograr la carga dinámica en tiempo real de entornos tridimensionales dentro del proyecto Galerías Virtuales 3D, para optimizar el rendimiento, la reducción de tiempos de carga y la implementación de un sistema flexible para la creación, almacenamiento y visualización de exposiciones digitales interactivas.

2. DESARROLLO TÉCNICO

El proyecto Galerías Virtuales 3D busca ofrecer una plataforma escalable y accesible para que cualquier miembro de la comunidad universitaria pueda crear y compartir su propia galería interactiva en web. Sin embargo, el desarrollo técnico enfrentó dos problemas principales.

Primero, reducir los tiempos de carga iniciales del interactivo, ya que los entornos tridimensionales contienen modelos complejos y texturas pesadas que afectan el rendimiento y aumentan el peso total del interactivo. Incluir todos los entornos disponibles dentro del interactivo implicaba una carga innecesaria de recursos, ya que cada usuario sólo requiere el entorno que haya seleccionado para su galería.

Segundo, diseñar un sistema eficiente para almacenar y recuperar dinámicamente las configuraciones de cada galería creada por los usuarios, con sus respectivas obras, fichas técnicas y disposición espacial, de forma que fuera fácil y rápido reconstruir las galerías creadas por los usuarios.

2.1 METODOLOGÍA

La metodología se estructuró en tres etapas: diseño, implementación y pruebas, lo que permitió ajustar decisiones técnicas de forma iterativa y progresiva.

2.2 DISEÑO

En esta etapa, se identificaron los principales requerimientos del sistema y se definieron las tecnologías para su implementación. Se consideraron los siguientes aspectos:

Se estableció un esquema de comunicación entre el interactivo y el servidor, mediante peticiones HTTP, para permitir la transferencia de datos de manera eficiente.

Se decidió emplear formatos ligeros para web, paquetes de recursos *(AssetBundles)* de Unity para la carga dinámica de los entornos, formato GLTF, ZIP (para GLTF con texturas y archivo binario) y GLB para los modelos, JPG y PNG para imágenes, MP3, WAV y OGG para audios, así como MP4 para videos.

Se decidió usar el formato JSON, un formato ligero optimizado para web, para almacenar de forma estructurada la información necesaria y poder reconstruir la galería al momento de abrirla.

Se definieron estrategias como la reducción de polígonos en modelos y precálculo de iluminación para mejorar el rendimiento.

- Uso de WebGPU y WebGL, aceleración gráfica en navegadores modernos para optimizar la experiencia.
- Las herramientas tecnológicas utilizadas se resumen a continuación en la Tabla 1.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.115 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 37 - 42

Tabla 1

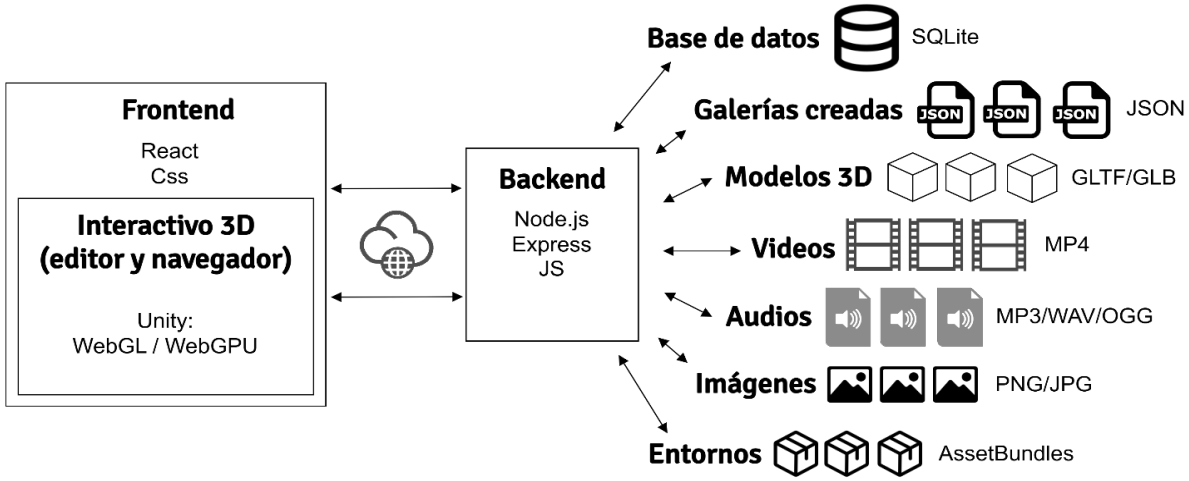
Tecnologías utilizadas en el desarrollo del sistema Galerías Virtuales 3D

Componente	Tecnología usada	Tecnología usada	Función principal
Motor 3D	*Unity*	*6.1* (6000.1.0f1)	*Desarrollo* del interactivo 3D y exportación WebGL y WebGPU
Interfaz web	*React*	*18.2.0*	*Plataforma* para incrustar el interactivo y gestionar el acceso
Servidor	*Node.js* + Express	*21.7.3* + 4.21.1	*Manejo* de peticiones HTTP, archivos y base de datos
Base de datos	*SQLite*	*5.1.7*	*Almacenamiento* de usuarios, galerías y obras

Como complemento a la Tabla 1, la Figura 1 ilustra la arquitectura del sistema Galerías Virtuales 3D, destacando cómo se integran los componentes tecnológicos descritos anteriormente.

Figura 1

Arquitectura de Galerías Virtuales 3D



2.3 IMPLEMENTACIÓN

La implementación del sistema se estructuró en tres componentes principales: el servidor, el interactivo 3D y la interfaz web. A continuación, se describe el proceso técnico seguido para su desarrollo e integración, las decisiones de arquitectura y los pasos necesarios para su reproducción.

- Escena base del interactivo en Unity: se utilizó Unity para construir la escena base del interactivo 3D, incluyendo únicamente los scripts de navegación, la interfaz gráfica y el sistema de carga dinámica.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.115 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 38 - 42

No se incluyeron entornos ni modelos de obras en el paquete inicial, con el fin de mantenerlo ligero y optimizado para la web. Esta separación permite que los recursos pesados se carguen sólo cuando son necesarios y mejorar así el rendimiento desde el arranque.

- Exportación de entornos como paquetes de recursos (AssetBundles): para abordar el problema del almacenamiento de los distintos espacios o entornos disponibles, se optó por utilizar AssetBundles, una solución nativa de Unity que permite empaquetar modelos, texturas y otros recursos como archivos externos comprimidos, cargables en tiempo de ejecución. Cada entorno fue configurado como un objeto prefabricado independiente y exportado como un paquete de recursos. Esta estrategia no sólo reduce el peso del paquete base del interactivo, sino que garantiza que únicamente se descargue el entorno específico que el usuario selecciona, manteniendo su configuración original y todos sus componentes intactos. Este enfoque permite escalar fácilmente el número de entornos nuevos disponibles.
- Desarrollo del servidor: se implementó un servidor en Node.js con Express; este servidor expone puntos finales del API REST para:

  - Cargar y descargar los archivos JSON con los metadatos de cada galería.

  - Gestionar y servir los paquetes de recursos de entornos, así como imágenes, audios, videos y modelos 3D asociados a las obras.

  - Registrar y consultar datos desde una base de datos SQLite, incluyendo usuarios, galerías y obras.

- Creación de la interfaz web: la interfaz fue desarrollada en React, lo que permite a los usuarios:

  - Crear nuevas galerías a través de un formulario.

  - Visualizar la lista de las galerías existentes.

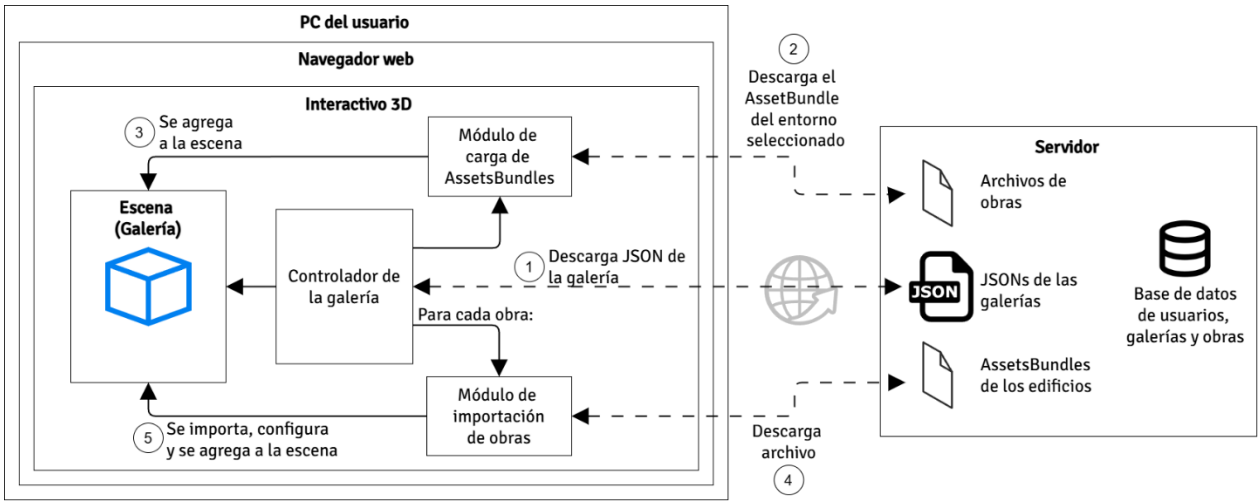
  - Acceder al interactivo en los diferentes modos (crear, editar o navegar) para una galería en específico.

Carga y deserialización en Unity: la reconstrucción de cada galería en tiempo real se logra mediante la descarga del archivo JSON desde el servidor y su deserialización en Unity. Este archivo contiene toda la información necesaria para ensamblar la escena: el entorno seleccionado, la lista de obras incluidas, sus posiciones, rotaciones, escalas, y fichas técnicas. A partir de esta información, el sistema descarga dinámicamente el paquete de recursos correspondiente al entorno seleccionado y lo integra en la escena; posteriormente descarga e instancia dinámicamente cada obra aplicando las propiedades definidas en el archivo JSON para su correcta visualización. Este proceso se ilustra en la Figura 2, que muestra la secuencia completa de ensamblado de una galería virtual en tiempo real.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.115 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 39 - 42

Figura 2

Ensamblado de una galería en tiempo real



Nota. Los números de la figura corresponden a: 1) El interactivo 3D solicita al servidor el archivo JSON correspondiente; 2) El módulo de carga de paquetes de recursos descarga el entorno; 3) Se agrega el modelo del entorno correspondiente a la escena interactiva; 4) Para cada obra registrada en la galería, el interactivo 3D solicita su archivo correspondiente al servidor; 5) Una vez descargadas, las obras son configuradas según la información proporcionada en el JSON de la galería e incorporadas al entorno 3D, permitiendo su visualización dentro de la galería virtual.

2.4 ESTRUCTURA DEL ARCHIVO JSON

Para almacenar y recuperar las galerías de forma eficiente, se utiliza un archivo JSON por galería. Este formato ligero y optimizado para la web permite que cada galería se reconstruya incluso tras ser editada posteriormente. Su estructura incluye referencias clave: entorno seleccionado, obras incluidas, parámetros espaciales y metadatos.

La Figura 3 muestra un ejemplo de esta estructura jerárquica, similar al enfoque descrito por Friston et al. (2017), donde el uso de JSON permite reconstruir dinámicamente escenas 3D desde bases de datos estructuradas. Al dividir los modelos en componentes individuales y cargarlos de forma selectiva, se mejora notablemente el rendimiento, especialmente en entornos WebGL.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.115 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 40 - 42

Figura 3

Estructura del archivo JSON para el almacenamiento de galerías con sus respectivas obras

```
{
  "fileName": "[nombre_archivo]",
  "id": "[identificador_único]",
  "name": "[nombre_galería]",
  "username": "[usuario_creador]",
  "enviromentId": [id_entorno_seleccionado],
  "description": "[descripción]",
  "startPosition": {
    "x": [posición_x],
    "y": [posición_y],
    "z": [posición_z]
  },
  "startRotation": {
    "x": [rotación_x],
    "y": [rotación_y],
    "z": [rotación_z],
    "w": [rotación_w]
  },
  "items": [
    {
      "id": "[identificador_único_item]",
      "name": "[nombre_item]",
      "type": "[tipo_item]",
      "position": {
        "x": [posición_x],
        "y": [posición_y],
        "z": [posición_z]
      },
      "rotation": {
        "x": [rotación_x],
        "y": [rotación_y],
        "z": [rotación_z],
        "w": [rotación_w]
      },
      "scale": {
        "x": [escala_x],
        "y": [escala_y],
        "z": [escala_z]
      },
      "metadata": {
        "source": "[fuente_dato]",
        "author": "[autor]",
        "date": "[fecha]"
      }
    }
  ]
}
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.115 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 41 - 42

2.5 PRUEBAS

Se realizaron pruebas funcionales y de rendimiento para validar la estabilidad y eficiencia del sistema:

- Verificación del funcionamiento en distintos navegadores.
- Validación del correcto almacenamiento y recuperación de las configuraciones de las galerías.
- Verificación de la correcta importación de modelos en el interactivo y su colocación.
- Validación de las interacciones en el interactivo.
- Evaluación de los cuadros por segundo durante la ejecución del interactivo.
- Evaluación de tiempos de carga con distintos tamaños de modelos y distintos entornos.

3. RESULTADOS

El enfoque modular permitió alcanzar mejoras tangibles en el rendimiento y flexibilidad del sistema. La carga dinámica de entornos mediante paquetes de recursos contribuyó directamente a la optimización del tamaño del interactivo y al rendimiento general, permitiendo cargar únicamente el entorno seleccionado por el usuario.

En pruebas realizadas durante el desarrollo, se comparó el peso del paquete completo, que incluía todos los entornos embebidos, contra una versión optimizada que excluye estos elementos y los distribuye como paquetes de recursos. La versión completa del interactivo alcanzaba tamaños superiores a 400 MB, mientras que el interactivo simplificado, que contiene sólo la lógica base e interfaz, se redujo a aproximadamente 80 MB, lo cual representa una disminución del 80% en el tamaño inicial de descarga. Esta diferencia se traduce directamente en menores tiempos de carga y mayor accesibilidad para los usuarios.

En cuanto al rendimiento en ejecución, se observó que, en equipos modernos con aceleración gráfica habilitada, especialmente aquellos con navegadores compatibles con WebGPU, el interactivo mantenía frecuencias de actualización superiores a los 60 FPS. Esta mejora se explica en parte porque "WebGPU proporciona un acceso más cercano al hardware moderno de la GPU [...] con mayor eficiencia y menor consumo de recursos del sistema" (Usta, 2024, p. 380), lo que permite aprovechar mejor la capacidad de los dispositivos actuales frente a WebGL. En contraste, en dispositivos con menor capacidad o navegadores con soporte limitado, la experiencia seguía siendo funcional, aunque con valores entre 25 y 45 FPS en escenas que incluían pocos modelos optimizados.

Sin embargo, se identificaron limitaciones cuando los usuarios cargan modelos 3D complejos sin compresión ni reducción de polígonos. Modelos de más de 10 MB o con geometría no optimizada provocaron caídas perceptibles en el rendimiento e incluso demoras en la carga. Esto resalta la importancia de contar en el futuro con un sistema de validación previa que alerte al usuario sobre el peso y complejidad de los modelos antes de integrarlos a una galería.

Por otro lado, se verificó la eficacia del esquema de ensamblado dinámico basado en archivos JSON, que permitió reconstruir correctamente las galerías en múltiples pruebas. El sistema logró esto utilizando los

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.115 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 42 - 42

archivos JSON generados, los cuales almacenan tanto la configuración del entorno como los datos de las obras, permitiendo su edición posterior sin pérdida de información o navegación.

En cuanto a la interoperabilidad, el interactivo se comportó de forma estable en navegadores modernos como Chrome, Edge y Firefox en Windows. No se identificaron errores críticos relacionados con la carga de recursos o la lectura de configuraciones, aunque falta continuar con pruebas en dispositivos móviles para validar la experiencia multiplataforma de forma completa.

4. CONCLUSIONES

La necesidad de reducir los tiempos de carga inicial y evitar paquetes pesados llevó a implementar una estrategia de carga dinámica en tiempo real para entornos tridimensionales en la plataforma de Galerías Virtuales 3D. Esta solución permitió excluir los entornos del núcleo del paquete base del interactivo y cargarlos según demanda del usuario, lo cual se tradujo en una experiencia más fluida. La solución permite escalar fácilmente la oferta de entornos virtuales disponibles sin impactar el rendimiento base del sistema.

La solución aplicada para tratar de optimizar los tiempos de carga en entornos interactivos, desarrollados en Unity para web, puede aplicarse en diversas situaciones para mejorar el rendimiento y la navegación fluida, así como el almacenamiento de datos en un archivo estructurado y ligero para almacenar información predefinida; no obstante, es aún más útil para almacenar información generada en tiempo de ejecución.

Un factor relevante es el número y características de las obras que agregue un usuario a su galería; queda pendiente agregar procesos que validen y limiten el peso, resolución de imágenes y número de vértices de los modelos 3D, con el objetivo de no sobrecargar la escena con imágenes o modelos tridimensionales muy pesados tanto en almacenamiento como en procesamiento gráfico.

REFERENCIAS

Friston, S., Fan, C., Doboš, J., Scully, T., & Steed, A. (2017). *3DRepo4Unity: Dynamic loading of version controlled 3D assets into the Unity game engine*. En *Proceedings of the 22nd International Conference on 3D Web Technology* (pp. 223–231). ACM. https://doi.org/10.1145/3055624.3075941

Usta, Z. (2024). WEBGPU: A NEW GRAPHIC API FOR 3D WEBGIS APPLICATIONS. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *48*(4/W9), 377–382. https://doi.org/10.5194/isprs-archives-XLVIII-4-W9-2024-377-2024

Zheng, Y., Merchant, A., Laninga, J., Xiang, Z. X., Alshaebi, K., Arellano, N., Romaniuk, H., Fai, S., & Sun, D. H. (2023). Comparison of characteristics of BIM visualization and interactive application based on WebGL and game engine. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, XLVIII-M-2-2023, 1671–1677. https://doi.org/10.5194/isprs-archives-XLVIII-M-2-2023-1671-2023

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116

Vol. 3, Núm. 3. julio-septiembre 2025, págs. 43 - 60

Encuesta de diagnóstico de diversidad estudiantil en la Facultad de Derecho

Información del reporte:

Para citar este reporte técnico:

Lira Jiménez et al. (2025). Encuesta de diagnóstico de diversidad estudiantil en la Facultad de Derecho. *Cuadernos Técnicos Universitarios de la DGTIC, 3* (3) páginas (43 - 60).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116

Laura Azucena Lira Jiménez
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
laura.lira@educatic.unam.mx
ORCID 0009-0007-6959-2939

Alan López de Jesús
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
alan.lopez@educatic.unam.mx
ORCID 0009-0008-1226-9775

Miguel Zúñiga González
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
mzuniga@unam.mx
ORCID 0009-0007-3305-5496

Resumen

Las encuestas digitales son una herramienta valiosa para recopilar información que contribuya al diseño de políticas institucionales orientadas a atender las necesidades de la comunidad universitaria. Cuando se recolecta información sensible, es fundamental que la implementación de las encuestas garantice la seguridad, privacidad y resguardo de los datos. Por ello, se optó por LimeSurvey, una herramienta de software libre que permitió almacenar los datos en infraestructura universitaria, configurar

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 44 - 60

roles y generar códigos de acceso para los estudiantes; además, se realizaron adecuaciones gráficas y modificaciones en las cadenas de texto para personalizar la encuesta según las necesidades específicas del proyecto. La aplicación piloto sirvió para verificar la disponibilidad del servicio, mientras que el despliegue final consiguió la cantidad necesaria de respuestas gracias a su formato digital, lo que evidenció su eficiencia en la recolección de datos. Los resultados muestran la viabilidad de LimeSurvey para proyectos académicos, con ventajas como el mantenimiento de la propiedad de los datos y su capacidad de adaptación a requerimientos particulares.

Palabras clave:

Encuesta digital, software libre, Limesurvey, privacidad.

Abstract

Digital surveys are a valuable tool for collecting information that contributes to the design of institutional policies aimed at addressing the needs of the university community. When collecting sensitive information, it is essential that survey implementation guarantees the security, privacy, and safety of the data. Therefore, LimeSurvey was chosen, an open-source software tool that allowed data to be stored on university infrastructure, roles to be configured, and access codes to be generated for students. Graphical adjustments and text string modifications were also made to customize the survey according to the specific needs of the project. The pilot application served to verify the availability of the service, while the final deployment achieved the necessary number of responses thanks to its digital format, demonstrating its efficiency in data collection. The results demonstrate the viability of LimeSurvey for academic projects, with advantages such as maintaining data ownership and its adaptability to specific requirements.

Keywords:

Digital survey, open-source software, Limesurvey, privacy.

1. INTRODUCCIÓN

En la UNAM, los procesos de diagnóstico institucional son fundamentales para comprender fenómenos como la diversidad, la inclusión y la equidad. Su propósito es generar información confiable que permita diseñar e implementar políticas orientadas a atender las necesidades de la comunidad universitaria. Entre las herramientas disponibles para este fin, las encuestas digitales se han consolidado como un recurso eficaz para la recolección de datos a gran escala, gracias al ahorro económico que representan en comparación con los cuestionarios en papel (Arroyo y Finkel, 2019).

Cuando los temas a abordar son especialmente sensibles —como la diversidad sexual, la identidad de género, la discriminación o la percepción de inclusión— es indispensable garantizar altos estándares de seguridad y privacidad durante el proceso de implementación de las encuestas en línea (Regmi et al., 2016). En este contexto, la elección de las herramientas tecnológicas y la ejecución de procesos y procedimientos no es trivial, porque deben enfocarse en preservar la calidad y confiabilidad de los datos obtenidos, al tiempo que garantizan la privacidad de los datos de quienes participan en los estudios.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 45 - 60

En este reporte, se subraya la importancia de utilizar soluciones de software libre, ya que permiten a la UNAM tener control del flujo de trabajo de la herramienta y de los datos que almacena, además de las siguientes ventajas (i Hernàndez, 2019, 41-54):

- personalizar vistas y extender funcionalidades gracias al acceso a su código fuente,
- sin costo en licencias o suscripciones,
- permite compartir experiencias de uso de manera comunitaria.

Asimismo, el software libre ayuda a incentivar el trabajo colaborativo y cooperativo, lo que facilita que se pueda adaptar a las necesidades del proyecto requerido (Valenzuela Urra et al., 2018). Esta característica se complementa con la integración de las actividades clave en la entrega de un servicio, con base en el marco de ITIL 4, para asegurar la calidad, continuidad, eficiencia y mejora continua al proporcionar el servicio.

La Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) impulsa diversas estrategias orientadas a fortalecer las funciones sustantivas de la Universidad mediante el uso de tecnologías. En DGTIC, se ha impulsado el uso de software libre como Moodle (los módulos de encuesta y cuestionario/examen) para la implementación de instrumentos de diagnóstico o encuestas con fines específicos, aprovechando su capacidad de personalización, la posibilidad de instalar esta aplicación en servidores institucionales y la posibilidad de adaptar el código o los esquemas de aprovisionamiento y despliegue a contextos particulares (Ramírez A. y Zuñiga M., 2024).

A mediados del año 2024, DGTIC atendió la solicitud de colaboración por parte de la Facultad de Derecho para implementar una encuesta en línea dirigida a estudiantes de licenciatura, con el objetivo de realizar un diagnóstico institucional en torno a temas de diversidad e inclusión. Dado el carácter sensible de los temas abordados, el proyecto exigía una solución tecnológica que garantizara el control sobre el almacenamiento y manejo de datos, permitiera validar la identidad de los usuarios a través de credenciales institucionales, y asegurara la disociación de las respuestas de los datos de usuario en el almacenamiento, recuperación y en el procesamiento de los resultados. Asimismo, era necesario personalizar la apariencia de la encuesta e intervenir en las cadenas de idioma de la aplicación para adaptar la experiencia de uso a los requerimientos específicos del proyecto.

En este contexto, se llevó a cabo un trabajo técnico especializado que incluyó el diseño, la configuración, las pruebas y la puesta en marcha de la encuesta de forma segura, eficiente y conforme a los requerimientos académicos. El proceso abarcó reuniones de análisis de requerimientos con las responsables del proyecto, la configuración del cuestionario y de los permisos de usuario, la personalización visual e idiomática del aplicativo, la realización de una prueba piloto y el seguimiento técnico continuo durante la aplicación final.

El objetivo de este reporte técnico es describir la implementación en la infraestructura institucional de la UNAM a partir de una encuesta digital masiva que permitiera garantizar la privacidad, el control de acceso y el tratamiento anónimo de las respuestas.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 46 - 60

2. METODOLOGÍA

El proyecto se desarrolló con el enfoque metodológico propuesto por el marco ITIL 4 (*Information Technology Infrastructure Library 4*), un enfoque ampliamente adoptado para la gestión eficiente y sistemática de servicios de tecnologías de la información (Zúñiga Arguedas, 2022; Palacios-Osma et al., 2017, 28). Este marco propone el concepto de *cadena de valor* como modelo del desarrollo de un servicio (Axelos, 2019, 52).

La cadena de valor del servicio es el conjunto de seis actividades clave interrelacionadas que una organización realiza para brindar un servicio valioso para su consumidor (Axelos, 2019, 53). A continuación, se describen estas actividades:

1. **Planificar.** El propósito de esta actividad es garantizar una comprensión compartida entre los interesados de la visión, el estado actual y la dirección de mejora del servicio, asegurando su alineación con los objetivos estratégicos de la institución.
2. **Involucrar.** Esta actividad busca asegurar una comprensión adecuada de los requerimientos del servicio por parte de las partes interesadas.
3. **Diseño y transición.** Su propósito es asegurar que el servicio cumpla con los requerimientos establecidos, es decir, con las expectativas acordadas con las partes interesadas.
4. **Obtener y/o Construir.** Esta actividad garantiza que los componentes del servicio estén disponibles cuando y donde se necesiten, y que cumplan con los estándares de calidad definidos.
5. **Entregar y dar soporte.** El objetivo de esta actividad es asegurar que los servicios se entreguen y respalden de manera efectiva, cumpliendo con los niveles acordados de calidad.
6. **Mejorar.** Esta actividad pone énfasis en la necesidad de contemplar la mejora continua de los servicios.

Para este proyecto, se adaptó el concepto de cadena de valor del servicio al contexto universitario. A continuación, se describen estas actividades tal como fueron aplicadas.

El resultado de la actividad de *Planificación* constituye las líneas generales de acción sobre las que se desarrollará el servicio, con las cuales se toman las decisiones fundamentales del proyecto (Kaiser, A., 2021, 134). En este sentido, el personal de DGTIC y las responsables académicas de la encuesta, de la Facultad de Derecho, definieron estos acuerdos fundamentales para el desarrollo del servicio. Se acordó, como objetivo general del proyecto, proporcionar el soporte tecnológico para realizar la encuesta digital de diagnóstico de diversidad estudiantil en la Facultad de Derecho.

La actividad *Involucrar* se realizó mediante reuniones con el equipo académico responsable del instrumento para recabar los requerimientos puntuales, lo que permitió acordar los objetivos específicos del servicio: 1) la protección de los datos sensibles que recolectaba la encuesta, 2) el uso de credenciales de acceso para asegurar que sólo los estudiantes de la Facultad de Derecho podían responder el cuestionario, 3) tratar las respuestas como anónimas y 4) realizar personalización visual y del texto de la aplicación.

La actividad de *Diseño y transición* consistió en la selección de la herramienta, mediante la cual se construyó un prototipo funcional en un ambiente de pruebas, que facilitó la revisión de las preguntas en

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 47 - 60

conjunto con las responsables académicas del proyecto; además de revisar el contenido de las preguntas, se revisó la navegación, se eligieron los tipos de preguntas a implementar, se adaptaron las indicaciones al entorno digital y se acordó la navegación y presentación del instrumento.

Sobre la actividad de *Obtener y construir*, a partir de la información recabada con el prototipo funcional, se construyó la encuesta en el ambiente de producción, con las configuraciones y personalizaciones necesarias, para asegurar el cumplimiento de los requerimientos acordados. También se llevó a cabo una prueba piloto con usuarios reales para identificar el desempeño de la encuesta en el momento de la ejecución.

Con respecto a la actividad de *Entregar y dar soporte*, la experiencia de la prueba piloto brindó la información necesaria para realizar el despliegue del servicio, junto con las acciones de soporte para los usuarios finales y acompañamiento a las autoridades durante el desarrollo del mismo.

La actividad de *Mejora* se aplicó a lo largo del proceso porque, en cada etapa, incluidas las pruebas, se permitía identificar puntos a optimizar, los cuales se incorporaron al diseño e implementación del servicio.

3. DESARROLLO TÉCNICO

La implementación de la encuesta se estructuró en cuatro etapas específicas: la selección de la herramienta, el diseño, el despliegue y la mejora continua. En cada una de las etapas, se trabajó en conjunto con el personal de la Facultad de Derecho para atender las necesidades requeridas.

3.1 SELECCIÓN DE HERRAMIENTA

En esta etapa, se realizó una valoración de las herramientas disponibles para implementar la encuesta. La Tabla 1 resume esta comparativa.

Tabla 1

Comparativa de herramientas para aplicar encuestas

Característica	LimeSurvey CE (Open Source)	Google Forms (Workspace)	Moodle (Quiz o questionnaire)	Nextcloud (Forms addin)	SurveyMonkey (Freemium)
Licenciamiento	Gratuito (GPLv2)	Gratuito con límites	Gratuito (GPL)	Gratuito (AGPLv3)	Freemium ($25/mes)
Alojamiento	Autohospedado	Nube de Google	Autohospedado	Autohospedado o en nube	Nube (EE.UU.)
Privacidad	Cumple LGPD/GDPR. Separa los datos de usuario de las respuestas.	Datos en servidores de Google fuera del territorio nacional	Control institucional	GDPR, CCPA, HIPAA, FERPA, COPPA y varios ISO	Cifrado básico

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 48 - 60

Característica	LimeSurvey CE (Open Source)	Google Forms (Workspace)	Moodle (Quiz o questionnaire)	Nextcloud (Forms addin)	SurveyMonkey (Freemium)
Personalización	CSS/JS, *plugins*	Plantillas y combinaciones limitadas	Integrado en LMS	CSS/JS y plantillas	Plantillas prefijadas. La extensión requiere costo adicional
Tipos de Preguntas	30+ (matriciales, lógicas)	10 básicas	15 (incluye SCORM)	5 básicas	15 (lógica condicional)
Análisis de Datos	SPSS, STATA,CSV	Solo CSV/Excel	Informes Moodle	Solo CSV	15 (lógica condicional)
Usabilidad	Curva de aprendizaje	Intuitivo	Requiere Moodle	Curva de aprendizaje	Interfaz clara
Mejor para	Encuestas personalizadas con propiedad de los datos.	Encuestas rápidas	Cursos en Moodle	Encuestas básicas	Encuestas comerciales

En la comparativa que muestra la Tabla 1, se incluyeron los cuestionarios de Moodle porque, en experiencias previas, se adaptaron para la aplicación de diagnósticos institucionales debido a su flexibilidad, control de accesos y mecanismos de almacenamiento de la información (Ramírez A. y Zuñiga M., 2024). Sin embargo, la encuesta de la Facultad de Derecho requería funcionalidades específicas como preguntas tipo matriz, condicionales con lógica avanzada y el almacenamiento de datos personales de las personas participantes, los cuales deben manejarse conforme a las disposiciones en materia de seguridad, transparencia y acceso a la información de la UNAM (Red TIC UNAM, 2024). Estos requerimientos resultaban difíciles de implementar adecuadamente en Moodle.

De manera paralela, se valoraron como alternativas los formularios de Google Workspace —por su facilidad de creación— y el complemento de formularios para Nextcloud, aplicación sobresaliente por su esquema de seguridad (Nextcloud, 2025) y que, a lo largo de su historia, por sus características de código abierto, recibe auditorías y reportes de vulnerabilidades de diferentes tipos de organizaciones (Albrecht, 2024; Niehage, 2020). Sin embargo, ambas opciones fueron descartadas por no ofrecer el nivel de personalización visual y textual que el proyecto requería.

Dado que se requería control sobre el almacenamiento y manejo de los datos recolectados, así como la personalización de la interfaz y del idioma, se optó por una herramienta de software libre alojada en la infraestructura institucional (i Hernàndez, J., 2019). En consecuencia, se descartó el uso de plataformas comerciales como SurveyMonkey o Google Forms.

Derivado del análisis comparativo, se identificaron las siguientes características que favorecieron el uso de LimeSurvey CE:

- Almacenamiento de los datos. Al tener una instalación propia, los datos de las encuestas se almacenan en servidores locales de la UNAM. Esto proporciona un control sobre la seguridad y privacidad de éstos, lo cual es crucial, especialmente si se maneja información sensible.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 49 - 60

- Personalización avanzada. LimeSurvey permite personalizar la apariencia de las encuestas y las cadenas de texto que muestran los formularios.
- Sostenibilidad y autonomía. Al tenerlo alojado internamente, la UNAM no depende de servicios de terceros, lo que permite al personal universitario gestionar la continuidad del servicio. No hay riesgo de que el servicio se vea afectado por cambios en las condiciones de uso o en la infraestructura de un proveedor.
- Actualización y documentación. Al ser de código abierto, LimeSurvey tiene una comunidad de usuarios y desarrolladores que mantiene el desarrollo y la documentación de la aplicación en diferentes idiomas, además de un foro donde se exponen dudas, escenarios de aplicación y alternativas de solución.
- Separación efectiva entre los datos de autenticación y las respuestas. LimeSurvey permite restringir el acceso a las encuestas mediante un código de acceso aleatorio (*token*) asociado a una cuenta de correo electrónico; no se recopila información adicional.
- Encuestas anónimas. La arquitectura de LimeSurvey contempla encuestas anónimas; en este caso, ni los administradores del sistema pueden vincular las respuestas con los datos de ingreso.

En relación con el último punto, cuando se habilita la opción de respuestas anónimas, tanto la fecha de envío de la respuesta como la fecha de finalización del *token* se registran con el valor 1980-01-01 00:00, independientemente de otras configuraciones. Además, la tabla correspondiente carece de un índice en la declaración de registros, lo cual impide asociar los datos del servidor web y las respuestas recolectadas. Esto previene, por ejemplo, que se pueda identificar un *token* en los registros del servidor al iniciar una encuesta, o que se intente deducir el orden de las respuestas a partir del orden, fecha y hora de uso de los *tokens* (LimeSurvey, 2025).

Es importante aclarar que el software LimeSurvey se distribuye bajo dos formas, LimeSurvey Cloud y LimeSurvey CE (Community Edition):

1. Limesurvey Cloud es un servicio proporcionado por LimeSurvey GmbH (la empresa que se creó en torno al software LimeSurvey) y la cual proporciona diversos servicios de pago como alojamiento, plantillas personalizadas, paquetes complementarios, soporte técnico, etc. (LimeSurvey, 2023).
2. LimeSurvey CE es el software basado en servidor web que se distribuye gratuitamente bajo la Licencia pública general GNU GPL v2.

La versión utilizada para la realización de la encuesta es la versión LimeSurvey CE, la cual, al ser una plataforma "basada en software libre, ofrece mayores posibilidades de personalización que otras aplicaciones, porque además de permitir la programación de nuevas funcionalidades al usuario avanzado, cuenta con comunidades de desarrolladores en todo el mundo." (Arroyo y Finkel, 2019, p. 43). Esta herramienta es muy potente no sólo para la creación de encuestas masivas, sino también para cuestionarios en donde se requiera recabar información sobre servicios específicos, así como adaptarlos, personalizarlos y tener un mejor control para quien administra los datos, algo que otras herramientas libres o propietarias no ofrecen, o bien, lo ofrecen a costos más elevados como se vio en la Tabla 1.

Otro factor determinante en la elección de la plataforma fue la posibilidad de utilizar este software para ofrecer un servicio de evaluación a distintas entidades universitarias que requieran implementar

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 50 - 60

encuestas con características similares o personalizadas. La herramienta permite realizar numerosas modificaciones para adaptarse a diversos proyectos, tanto de servicios externos como de encuestas o formularios destinados a procesos internos del Departamento de Servicios Tecnológicos para la Educación, área de la DGTIC a cargo de este proyecto.

3.2 DISEÑO

Se trabajó de manera colaborativa con las responsables académicas de la encuesta a través de reuniones recurrentes, en las que se revisó y ajustó el contenido del cuestionario, se definieron las funcionalidades a implementar y se acordaron los criterios clave para su aplicación. Entre los acuerdos alcanzados destacan los siguientes:

- Se propuso un mecanismo para asegurar que únicamente alumnos de la Facultad de Derecho pudieran responder la encuesta, y que cada persona lo hiciera sólo una vez. Para ello, se utilizó el número de cuenta como código de acceso (*token*), funcionalidad nativa de LimeSurvey.
- Se generaron *tokens* ficticios para realizar pruebas de navegación y funcionalidad.
- Se acordó que las respuestas serían disociadas de los números de cuenta para garantizar así el tratamiento anónimo de los datos.
- Se identificaron los elementos que requerían personalización tanto en las cadenas de idioma como en el diseño visual de la encuesta.

Como primer paso, se recibió el cuestionario en formato de texto. A partir de este documento, se revisaron los tipos de preguntas para asegurar su compatibilidad con LimeSurvey o, en su caso, adaptarlas a los formatos disponibles en la plataforma. También se identificaron aquellas preguntas cuya visibilidad dependía de respuestas previas, así como las instrucciones necesarias, su extensión y el estilo tipográfico requerido.

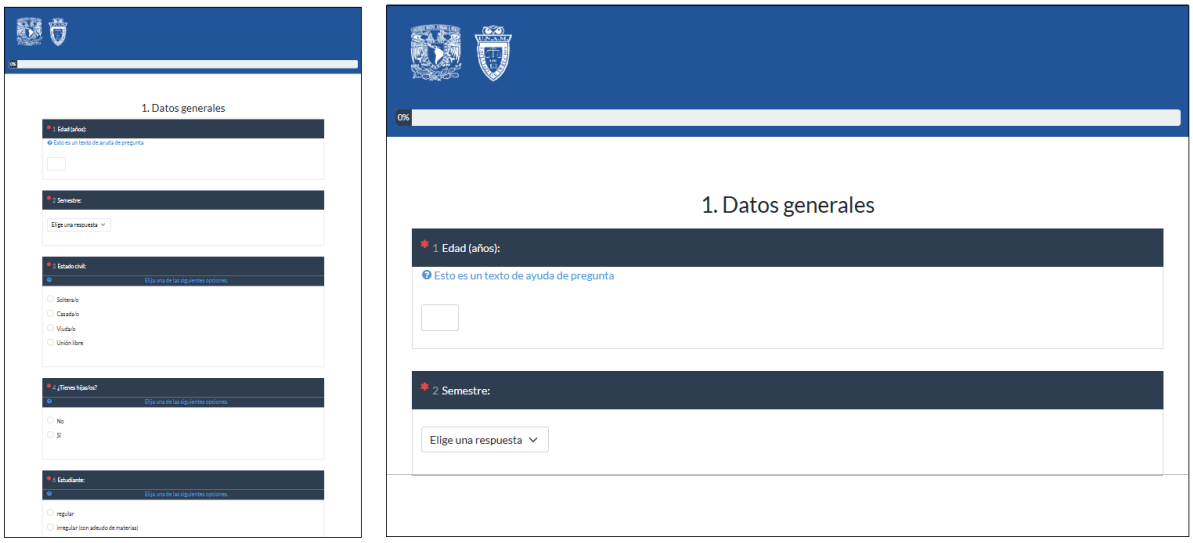
Dado que esta versión inicial del cuestionario fue concebida para una aplicación analógica, se realizaron observaciones y sugerencias para adaptarla a un entorno digital. También se propuso que la encuesta considerara las siguientes dimensiones de calidad: precisión, credibilidad, comparabilidad, interpretabilidad, relevancia, accesibilidad, puntualidad, plenitud y coherencia (Cea D'Ancona, 2022).

Posteriormente, se presentó un prototipo funcional con personalización visual, el cual fue revisado en conjunto con el equipo académico. Como resultado de esta evaluación, como se observa en la Figura 1, se ajustaron los textos de ayuda en algunas preguntas para optimizar su visualización tanto en dispositivos móviles como teléfonos celulares y tabletas.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 51 - 60

Figura 1

Prototipo de encuesta adaptada en celulares y tabletas



3.3 CREACIÓN

Durante esta fase, se llevaron a cabo la instalación y configuración de la plataforma LimeSurvey CE en su versión 6.12; ésta se desplegó en un servidor administrado en la DGTIC, utilizando una máquina virtual con especificaciones de 2 núcleos y 4 GB de RAM, bajo el sistema operativo Rocky Linux 8.10. Se configuraron roles de acceso diferenciados para proteger los permisos.

Una vez instalada la plataforma, se realizó la creación de la encuesta y se configuraron las siguientes características:

- Título del formulario
- Formato de fecha
- Marca decimal
- Descripción de introducción
- Idioma de la encuesta
- Mensaje de despedida
- Correo de soporte técnico
- Tema gráfico a utilizar
- Roles y permisos para permitir la colaboración y el monitoreo de la encuesta

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 52 - 60

Para la parte de presentación de la encuesta, se configuraron los siguientes parámetros de la sección de mostrar:

- Cuando una pregunta está sin respuesta
- Número de preguntas en la encuesta
- Código de la pregunta
- Pantalla de bienvenida
- Barra de progreso

Por otro lado, se habilitó la opción "Permitir navegar hacia atrás" con el fin de que las y los estudiantes pudieran modificar respuestas en páginas anteriores sin perder su progreso en la encuesta.

Para asegurar que quienes respondieran la encuesta fueran efectivamente alumnos de la Facultad de Derecho, y al mismo tiempo evitar respuestas duplicadas por parte de un mismo participante, se configuró un sistema de control de acceso, para lo cual se utilizó el número de cuenta del estudiante como código de ingreso a la encuesta.

En LimeSurvey, estos códigos se gestionan a través del sistema de *tokens* (también conocidos como códigos de acceso o de invitación), los cuales son códigos únicos asignados a cada participante. Su función es controlar quién puede responder la encuesta y cuántas veces lo puede hacer.

Los *tokens* fueron generados a partir de la base de datos de estudiantes proporcionada por la Facultad, lo que garantizó que cada estudiante tuviera acceso individualizado y pudiera participar una sola vez.

Otro requerimiento importante fue la personalización visual de la encuesta. Para ello, se creó un nuevo tema basado en el tema predeterminado Bootstrap. Este tema derivado fue renombrado como "tema Derecho" y se le aplicaron modificaciones en el código CSS y HTML para adaptarlo a la identidad visual de la entidad. En la Figura 2, se observa la sección de edición del tema derivado.

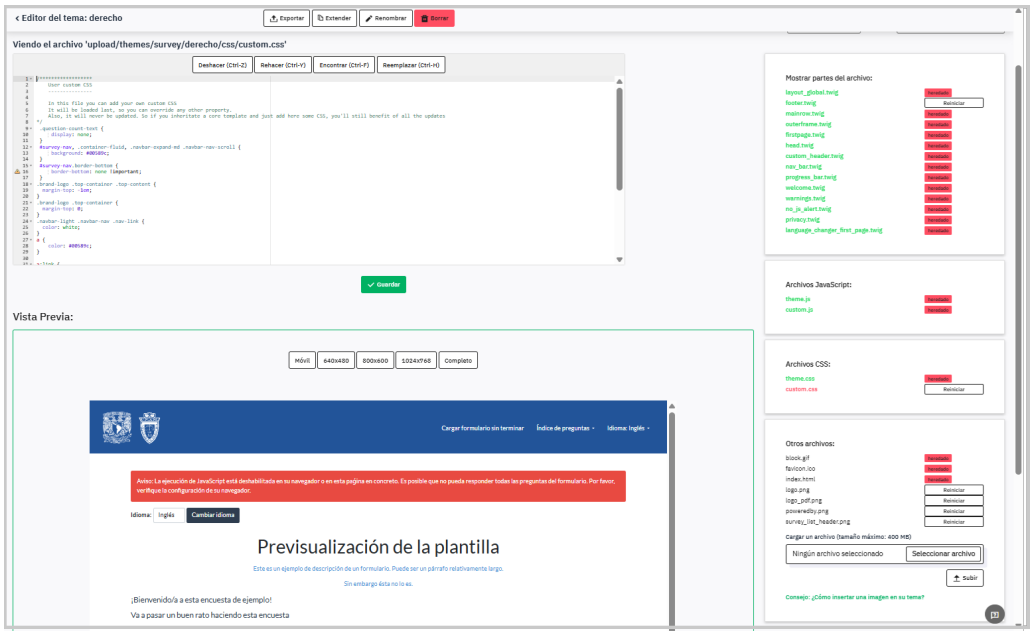
Además, se incorporaron los logotipos oficiales de la DGTIC y de la Facultad de Derecho en el encabezado, así como el ícono de la página (favicon), ajustando sus dimensiones y formato para cumplir con los lineamientos de identidad gráfica institucional.

Como parte fundamental del tratamiento de los datos personales, se modificó también el pie de página para incluir el aviso de privacidad de la DGTIC, el cual permaneció visible durante la aplicación de la encuesta.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 53 - 60

Figura 2

Edición y modificación del tema derivado



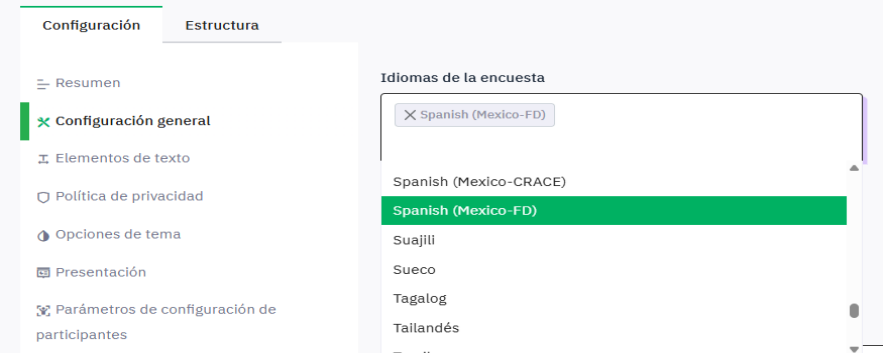
Dado que algunas secciones de la encuesta requerían mensajes específicos para las personas participantes, fue necesario modificar las cadenas de texto de la aplicación. LimeSurvey utiliza GNU Gettext como mecanismo para traducir su interfaz a diferentes idiomas; se aprovechó esta característica para implementar un idioma personalizado. Para ello, se descargó el archivo de idioma español de México desde el sitio oficial de LimeSurvey y, posteriormente, se modificó la traducción con la herramienta Poedit: el resultado fue un archivo compilado (.mo) con la traducción personalizada.

Dentro de la aplicación, en el directorio *locale*, se creó una carpeta para alojar la traducción personalizada y se añadió la declaración del nuevo idioma en *application/helpers/surveytranslator_helper.php.* Finalmente, dentro de las configuraciones generales de la encuesta, se seleccionó el idioma personalizado (véase Figura 4).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 54 - 60

Figura 4

Selección de idioma personalizado

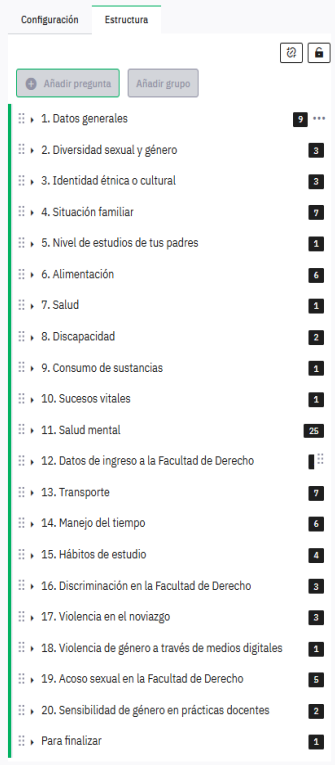


Aunque este procedimiento se realizó sobre una encuesta aún inactiva, cabe destacar que también puede aplicarse a encuestas activas sin interrumpir su funcionamiento ni afectar los enlaces o respuestas existentes.

El cuestionario se integró con 95 preguntas agrupadas en 20 secciones, ver Figura 5.

Figura 5

Grupos de preguntas del cuestionario



https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 55 - 60

Se utilizaron los siguientes 8 tipos diferentes de preguntas:

1. Entrada numérica: Permite que el usuario ingrese un solo valor numérico (entero o decimal).
2. Entrada numérica múltiple: Con varias subpreguntas, cada una con su propio campo numérico.
3. Lista (desplegable): Presenta una lista de opciones en un menú desplegable.
4. Lista (radio): Muestra una lista de opciones con botones de radio y sólo se puede elegir una.
5. Matriz: Tabla con varias subpreguntas (filas) y varias opciones (columnas) con botones de selección única.
6. Matriz de escala dual: Como una matriz, pero cada fila tiene dos escalas de respuesta.
7. Opción múltiple: Permite seleccionar más de una opción (*checkbox*).
8. Texto largo libre: Caja de texto para que el usuario escriba libremente una respuesta larga.

Algunas preguntas requirieron el uso de una condición de visibilidad, de manera que se mostró una pregunta sólo si se había seleccionado una respuesta previa. En la Tabla 2, se ejemplifican dos preguntas involucradas con una condición de visibilidad:

Tabla 2

Ejemplo de preguntas que requieren una condición de visibilidad

Código	Pregunta	Respuestas	Condición de visibilidad
s01p04	¿Tienes hijas/os?	AO01='No'; AO02='Sí'	
s01p05	¿Cuántos hijas/os?		((s01p04.NAOK == "A002"))

Nota. s01p04: es el nombre o código de la pregunta. LimeSurvey usa estos códigos para referirse a preguntas específicas.
.NAOK: es un modificador que significa "No Answer OK". Permite que la expresión se evalúe incluso si no hay una respuesta todavía.
= = "A002": es una comparación lógica que, en este caso, pregunta si la respuesta seleccionada por el usuario a la pregunta s01p04 fue la opción con código "A002".

Entonces, la expresión completa ((s01p04.NAOK == "A002")) significa: *Si* la persona seleccionó la opción con código A002 en la pregunta s01p04 *entonces* muestra la pregunta s01p04.

Las condiciones se pueden añadir en las configuraciones generales de la pregunta; si se observa la sección "Condición" en la Figura 6, se notará que se agregó la sintaxis descrita anteriormente.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 56 - 60

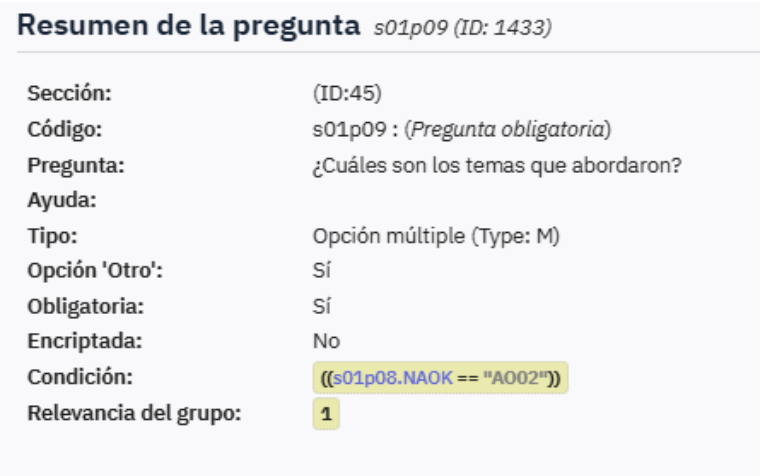
Figura 6

Condición de pregunta

En la Figura 7, se muestra el resumen de una pregunta, donde el penúltimo dato en la figura es una condición. Ésta es una forma de identificar si una pregunta cuenta con una condición.

Figura 7

Resumen de pregunta condicional



https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 57 - 60

El uso de un pilotaje antes de lanzar el servicio es de gran utilidad, ya que permite determinar que el servicio está listo para su despliegue (Alarcón y García, 2018). Por ello, se llevó a cabo una aplicación piloto de la encuesta con un grupo de 40 estudiantes; se realizó en un aula de cómputo de la Facultad de Derecho bajo la supervisión de las responsables académicas de la encuesta. Derivada de esta aplicación, se recibió retroalimentación cualitativa que permitió determinar que el servicio estaba listo para su despliegue.

3.4 DESPLIEGUE Y SOPORTE

La encuesta fue instrumentada para su aplicación institucional en infraestructura de la DGTIC, bajo supervisión de personal del Departamento de Servicios Tecnológicos para la Educación y las personas designadas de la Facultad de Derecho. En la fecha convenida, se activó el instrumento y se habilitó el acceso a los usuarios previamente definidos.

Se realizó un monitoreo diario del avance de las respuestas a través del panel correspondiente en LimeSurvey, lo que permitió dar seguimiento oportuno al desarrollo de la recolección de datos. Asimismo, se brindó atención y solución a las incidencias reportadas por el equipo académico, asegurando el funcionamiento de la herramienta.

Como parte del acompañamiento, se impartieron sesiones de capacitación dirigidas a las responsables académicas del proyecto, con el objetivo de facilitar el uso de la plataforma para el monitoreo y la descarga de resultados. Asimismo, se elaboró un manual de usuario en el que se documentaron los procedimientos, destinado específicamente a dicho perfil académico.

Junto a estas acciones, se documentaron diversos aspectos técnicos en la base de conocimiento del área responsable en la DGTIC. En particular, LimeSurvey requiere PHP 7.4 y también tiene soporte para PHP 8.0 a 8.2. Se habilitó *short_open_tag* en el php.ini como se recomienda en la documentación oficial (LimeSurvey, 2024).

Durante las pruebas realizadas, se observaron avisos por límite en el número de variables procesadas. Ante ello, se incrementó el valor de *max_input_vars* de PHP de 5000 —el mínimo requerido por PHP 8.0 para aplicaciones web con componentes reactivos, como Moodle 4.x (Moodle.org, 2023)— a 10000, lo cual tuvo un efecto positivo. Cabe señalar que, previamente, se evaluó el impacto en el consumo de memoria derivado de dicho ajuste.

En cuanto al procedimiento para la personalización visual de la plataforma, se decidió utilizar el módulo de creación de temas derivados, utilizado en los cuestionarios individuales, que forma parte de LimeSurvey. Al seleccionar «temas» en el menú principal, se puede «derivar» o tomar como referencia alguno de los archivos que componen algún tema incluido en LimeSurvey, se puede adaptar el CSS, el Javascript o las plantillas generales a contextos particulares. Se derivó el tema a partir del predeterminado y se adaptaron colores, se retiraron algunos elementos de la plantilla y se agregó el pie de página institucional.

Los procedimientos de personalización también se agregaron a la base de conocimientos del área responsable en la DGTIC, como documentación que tiene como propósito agilizar y fortalecer futuras implementaciones de instrumentos similares.

Al concluir el periodo de aplicación, se entregó el archivo con los resultados anónimos en formato CSV y se procedió a llenar el acta de cierre del proyecto, lo cual formalizó la finalización del proceso.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 58 - 60

3. RESULTADOS

La implementación de la encuesta digital logró cumplir con los objetivos establecidos en la fase de planeación, particularmente, en lo relativo a la recolección de datos sensibles con altos estándares de privacidad, anonimato y control institucional. La plataforma LimeSurvey, instalada en servidores de la DGTIC, permitió configurar un instrumento con preguntas condicionales y con validaciones específicas, personalización visual y del idioma, restricciones de acceso por credenciales y mecanismos de anonimización.

Con este trabajo, se obtuvo un instrumento digital plenamente funcional, que fue aplicado de forma segura y sin interrupciones durante el periodo establecido. Durante la aplicación de la encuesta, 433 estudiantes completaron el cuestionario, superando así la muestra requerida de 400 personas, según lo solicitado por la Facultad de Derecho.

Algunos datos relevantes de la implementación del cuestionario en línea son los siguientes: el tiempo promedio para responder la encuesta fue de 32 minutos; las franjas horarias con mayor número de respuestas fueron de 14:00 a 15:00 horas y de 19:00 a 20:00 horas. Otro aspecto destacable fue la eficacia del uso de tokens como validador, lo que permitió evitar la duplicidad de respuestas por parte de un mismo usuario.

Desde una perspectiva metodológica, el modelo de la cadena de valor del servicio de ITIL v4 permitió estructurar y evaluar las actividades clave del proceso. Esta orientación facilita la identificación de decisiones técnicas, como la elección de LimeSurvey sobre otras herramientas, así como la justificación del diseño del servicio en función de requerimientos institucionales. Otro punto importante a mencionar es la documentación de los procesos técnicos para asegurar la reproducibilidad del servicio en diferentes encuestas.

El análisis de resultados muestra que el uso de tecnologías de software libre instaladas localmente permite cumplir con exigencias estrictas de privacidad y control de datos, especialmente en contextos universitarios donde los principios de autonomía y confidencialidad son fundamentales.

4. CONCLUSIONES

La necesidad de aplicar un diagnóstico institucional sobre diversidad e inclusión en la Facultad de Derecho evidenció una problemática compleja: ¿cómo obtener datos sensibles garantizando su privacidad? El proyecto logró atender esta necesidad mediante la implementación de una encuesta digital con software libre, instalada y gestionada desde la infraestructura tecnológica de la UNAM, asegurando la calidad del proceso y los datos generados.

La experiencia muestra la importancia de realizar pruebas piloto para ajustar contenidos, funcionalidades y flujos de navegación antes de la aplicación final.

Los hallazgos confirman que es posible ofrecer un servicio tecnológico robusto y personalizable, alineado con los objetivos estratégicos de la Universidad, sin comprometer la privacidad de los participantes. La orientación metodológica basada en ITIL v4 permitió identificar, construir, dar guía, orden y mejorar cada fase del proyecto desde una lógica de servicio, así como documentar tanto los logros como las áreas de mejora.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 59 - 60

Derivado del éxito en la implementación de la Encuesta de diagnóstico de diversidad estudiantil en la Facultad de Derecho, queda para trabajos futuros explorar medios de difusión dirigidos a otras entidades universitarias, con el fin de promover los beneficios que ofrece LimeSurvey, una herramienta de software libre que puede favorecer a más proyectos e iniciativas universitarias.

REFERENCIAS

Alarcón González, F. J., & García Hípola, G. (2018). *Entrevistas Online. La encuesta a través de Internet: obstáculos, beneficios, y lecciones aprendidas*. 14. https://hdl.handle.net/10481/101546

Albrecht, M. R., Backendal, M., Daniele Coppola, D. (2024). Share with Care: Breaking E2EE in Nextcloud. *Infosec Applied Crypto and Education*, Departement Informatik. Eidgenössische Technische Hochschule Zürich (ETH Zurich), Switzerland https://eprint.iacr.org/2024/546

Arroyo Menéndez, M., & Finkel, L. (2019). Encuestas por Internet y nuevos procedimientos muestrales. *Panorama Social*, (30), 41-53. https://www.funcas.es/wp-content/uploads/Migracion/Articulos/FUNCAS_PS/030art04.pdf

Axelos Limited. (2019). *ITIL 4 Foundation Revision Guide*. Stationery Office.

Cea D'Ancona, M.ª. Á. (2022). Calidad, confianza y participación en encuestas. *PAPERS*, *107*(4), 27. https://doi.org/10.5565/rev/papers.3074

i Hernàndez, J. M. (2019). *Software libre: técnicamente viable, económicamente sostenible y socialmente justo* (1st ed.). España: Infonomia.

Kaiser, A. K. (2021). *Become ITIL® 4 Foundation Certified in 7 Days: Understand and Prepare for the ITIL Foundation Exam with Real-life Examples*. Apress.

LimeSurvey. (2025). Anonymized responses. Participant Settings. *LimeSurvey Manual*. https://www.limesurvey.org/manual/Participant_settings#Anonymized_responses

LimeSurvey. (2024). Instalación - LimeSurvey CE. *LimeSurvey Manual*. https://www.limesurvey.org/manual/Installation_-_LimeSurvey_CE/es

LimeSurvey. (2023). *LimeSurvey PRO y LimeSurvey CE*. LimeSurvey. https://www.limesurvey.org/manual/manual/LimeSurvey_PRO_vs_LimeSurvey_CE/es

Moodle.org. (2023). Moodle 4.1 Requirements. *Moodle Releases*. https://moodledev.io/general/releases/4.1

Nextcloud. (2025). *Security and authentication*. https://nextcloud.com/secure/

Niehage, K. (2020). Cryptographic Vulnerabilities and Other Shortcomings of the Nextcloud Server Side Encryption as implemented by the Default Encryption Module. *Cryptology ePrint Archive*. 1439. https://eprint.iacr.org/2020/1439.pdf

Palacios-Osma, J. I., Rodríguez-Guzmán, J. L., & García-Ramírez, C. X. (2017). Modelo de gestión de servicios ITIL para E-learning. *Educación en Ingeniería*, *12*(23), 28-34. 10.26507/rei.v12n23.684

Ramírez Bedolla, A. M., & Zúñiga González, M. (2024). Experiences of application of digital skills diagnostic in UNAM's schools. *EDULEARN24 Proceedings*, 6717-6722. https://library.iated.org/view/RAMIREZBEDOLLA2024EXP

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.116 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 60 - 60

Red TIC UNAM. (2024). III. Marco legal o normativo. *Recomendaciones para el almacenamiento de información*. https://www.red-tic.unam.mx/recomendaciones-almacenamiento#iii-marco-legal-o-normativo

Regmi, P. R., Waithaka, E., Paudyal, A., Simkhada, P., & van Teijlingen, E. (2016). Guía para el diseño y aplicación de encuestas de cuestionario en línea. *PubMed Central*, *4*(6). https://pmc.ncbi.nlm.nih.gov/articles/PMC5506389/

Valenzuela Urra, C., Reyes Lillo, D., & Oliveros Castro, S. (2018). Introducción: *Software* libre y código abierto: experiencias innovadoras en bibliotecas y centros de información. *Palabra Clave*, *8*(1), 2. https://doi.org/10.24215/18539912e054

Zúñiga Arguedas, E. (2022). Modelo de gestión organizacional basado en ITIL 4 - Prácticas de Servicios y su aporte a los sistemas de información para toma de decisiones. *InterSedes*, *23*(48), 21. https://doi.org/10.15517/isucr.v23i48.50034

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 61 - 80

Despliegue de OpenStack mediante Kolla-Ansible: una solución modular, automatizada y escalable para infraestructuras cloud

Información del reporte:

Para citar este reporte técnico:

Mares Mendoza, E. (2025). Despliegue de OpenStack mediante Kolla-Ansible: una solución modular, automatizada y escalable para infraestructuras cloud. *Cuadernos Técnicos Universitarios de la DGTIC, 3* (3) páginas(61 - 80).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117

Enrique Mares Mendoza

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Universidad Nacional Autónoma de México

enrique.mares@unam.mx

ORCID: 0009-0008-5529-0080

Resumen

Se analizó la posibilidad de implementar una infraestructura de nube, basada en software libre, en el Centro de Datos de la DGTIC de la UNAM, utilizando una solución que permitiera reducir costos operativos y dependencia de proveedores. Por lo tanto, se realizó una comparación de distintas herramientas de despliegue, para la que se consideraron criterios como facilidad de instalación, escalabilidad, automatización, mantenimiento y adecuación a entornos productivos. El análisis incluyó cinco enfoques distintos de despliegue, implementación manual y el uso de herramientas automatizadas reconocidas en la comunidad de *OpenStack*. Como resultado, se identificó que *Kolla-Ansible* ofreció un equilibrio entre complejidad y eficiencia, al integrar tecnologías de automatización y contenedores que permitieron una instalación modular, reproducible y segura. Si se compara con *OpenStack-Ansible*, TripleO o *DevStack*, demostró mayor estabilidad, menor carga de configuración inicial y facilidad para escalamiento de recursos. La prueba de despliegue con *Kolla-Ansible* validó su capacidad para reducir la intervención manual, minimizar errores humanos y agilizar los tiempos de implementación sin comprometer la disponibilidad del entorno. Se concluyó que, para infraestructuras orientadas a producción con requerimientos de escalabilidad, disponibilidad y gestión simplificada, esta herramienta

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 62 - 80

representa una solución robusta y estratégica que favorece la administración eficiente de servicios en la nube.

Palabras clave:

Openstack, Kolla-ansible, cloud, IaaS, Ansible.

Abstract

The feasibility of implementing an open-source cloud infrastructure at the UNAM's DGTIC Data Center was analyzed, utilizing a solution aimed at reducing operational costs and vendor dependency. Therefore, a comparison of various deployment tools was conducted, considering criteria such as ease of installation, scalability, automation, maintenance, and suitability for production environments. The analysis included five distinct deployment approaches, manual implementation and the use of automated tools recognized within the OpenStack community. As a result, Kolla-Ansible was identified as offering a balance between complexity and efficiency by integrating automation and container technologies, enabling a modular, reproducible, and secure installation. Compared to OpenStack-Ansible, TripleO, or DevStack, it demonstrated greater stability, lower initial configuration overhead, and easier resource scaling. The deployment test with Kolla-Ansible validated its ability to reduce manual intervention, minimize human errors, and streamline deployment times without compromising environment availability. It was concluded that for production-oriented infrastructures with scalability, availability, and simplified management requirements, this tool represents a robust and strategic solution that promotes efficient cloud service administration.

Keywords:

OpenStack, Kolla-Ansible, cloud, IaaS, Ansible.

1. INTRODUCCIÓN

Hoy en día, las tecnologías en la nube se han convertido en uno de los soportes más importantes de las infraestructuras tecnológicas modernas. *OpenStack* es ya una de las soluciones líderes para nubes privadas en este contexto. Gracias a su flexibilidad, escalabilidad y alto grado de personalización, es una alternativa muy útil para las entidades que buscan mejorar la optimización autónoma de la gestión de sus recursos tecnológicos. Bravo Roldán define *OpenStack* como una "plataforma de computación en la nube de código abierto para la creación tanto de nubes públicas como privadas que permite funcionalidad de Infraestructura como Servicio (IaaS)" (Bravo Roldán, L. A., 2022).

En este caso, *OpenStack* fue implementado en el Centro de Datos de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC), a través de un proveedor externo con servicios de soporte, para garantizar el servicio que se ofrece a las dependencias de la UNAM. Sin embargo, los altos costos anuales relacionados con el soporte llevaron a considerar la implementación de una versión *open-source* de *OpenStack*.

Se realizó una investigación donde se identificó que la principal forma de instalación que se encuentra en la documentación de *OpenStack* es desplegándolo manualmente, lo cual es un proceso que consume mucho tiempo y requiere tanto un profundo conocimiento técnico como una atención meticulosa a

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 63 - 80

los detalles en la instalación. Se analizó la implementación de *OpenStack*, ya que requiere configurar manualmente cada servicio que conforma a *OpenStack* desde *Nova*, que es el servicio de cómputo de la nube responsable de administrar el ciclo de vida de las instancias; *Neutron,* encargado de la red y conectividad; *Cinder,* que se encarga de proporcionar almacenamiento en bloques para las instancias; y *Keystone,* que gestiona la autenticación autorización e identidad, por nombrar algunos, para lo cual es necesario saber cómo funcionan juntos. Además, la falta de automatización aumentó el riesgo de inconsistencias, lo que dificulta la escalabilidad y el mantenimiento posterior. La gestión manual de actualizaciones y compatibilidades entre versiones también representa un desafío importante, por los riesgos de generar interrupciones en los servicios.

Para solucionar este problema, se analizaron las herramientas de despliegues automatizadas así como se identificaron las ventajas y desventajas de estas herramientas: destacó la herramienta de *Kolla-ansible,* ya que cubre las necesidades del Centro de Datos de la DGTIC.

El objetivo de este estudio es verificar el uso de *Kolla-Ansible* como herramienta clave en la implementación de un clúster de *OpenStack*, destacando su capacidad para simplificar y automatizar el despliegue de infraestructuras de nube en entornos de producción. Se busca evaluar *Kolla-ansible*, su eficiencia en la configuración de componentes críticos, como redes, almacenamiento y alta disponibilidad, así como su adaptabilidad para escalar en comparación con las demás herramientas de despliegue.

2. DESARROLLO TÉCNICO

2.1 PROPUESTA DE SOLUCIÓN

El cambio técnico en la implementación de O*penStack* ha sido posible gracias a la innovadora fusión de dos tecnologías fundamentales en la construcción de *Kolla-Ansible*: *Docker* y *Ansible*. Esta combinación funciona como un sistema modular y eficiente; cada servicio de *OpenStack* está en su propio contenedor, ligero y replicable, gracias a *Docker*, y *Ansible* se encarga de desplegarlos y configurarlos mediante *scripts* declarativos. Esto no sólo facilita la instalación, sino que también la hace consistente y escalable en entornos de nube complicados.

Para explicar este concepto, se invita a imaginar un sistema en el que cada servicio es encapsulado, en este caso en un contenedor de *Docker,* diseñado para realizar una tarea específica de manera precisa, mientras que una herramienta centralizada como *Ansible* coordina el funcionamiento de todos los contenedores. Esto da lugar a una infraestructura eficiente y flexible, capaz de adaptarse a las necesidades cambiantes de las organizaciones modernas, alineándose con tendencias globales como GitOps, que es una metodología de gestión de infraestructura a través de Git y la Infraestructura como Código (IaC). Según la documentación oficial de *Kolla*, "La misión de *Kolla* es proporcionar contenedores listos para producción y herramientas de implementación para operar nubes *OpenStack*" (*OpenStack Foundation*, 2019).

2.2 METODOLOGÍA

La relevancia de analizar el impacto técnico de *Kolla-Ansible* surge cuando se compara con una instalación manual de cada servicio de *OpenStack* o con otras herramientas alternativas de implementación como TripleO, *OpenStack-Ansible* y *DevStack*. Como una plataforma de computación en la nube de *open-source*,

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 64 - 80

OpenStack necesita soluciones efectivas de instalación para ser utilizado en entornos de producción y desarrollo. Estas herramientas son críticas para simplificar la configuración, minimizar errores y acelerar los tiempos de implementación.

Como se indica en el estudio presentado por Gudipati y Mithra, "las herramientas del marco de gestión del ciclo de vida (LCMT) ofrecen al administrador de *OpenStack* una forma sencilla de implementar, configurar y gestionar la plataforma en la nube" (Gudipati, S. V., & Mithra, T. V., 2022), por lo que es necesario identificar las herramientas más apropiadas que puedan facilitar la administración de esta tecnología.

Para llevar a cabo este análisis, se utilizó una metodología comparativa, que se centra en examinar y contrastar diferentes alternativas según criterios específicos. Este enfoque permite identificar ventajas, desventajas y características particulares que hacen más apropiada cada herramienta dependiendo de las necesidades o demandas específicas. La metodología incluye la evaluación técnica de las herramientas, su adecuación a distintos contextos (producción, desarrollo, pruebas, etc.) y la presentación de una tabla comparativa que resume las diferencias más relevantes.

Se seleccionaron *Kolla-Ansible*, *OpenStack-Ansible*, TripleO, *DevStack* y la instalación manual como las principales formas de despliegue de *OpenStack*. Estas opciones fueron elegidas por su amplio uso en la comunidad, su implementación en entornos de desarrollo, prueba y producción, así como por contar con soporte y documentación oficial que permite una comparación fundamentada. Cada una ofrece diferentes niveles de automatización, complejidad y adecuación según el caso de uso. A continuación, se describen sus principales características.

2.3 KOLLA-ANSIBLE

Kolla-Ansible despliega los servicios de *OpenStack* mediante contenedores *Docker*. Según Vainio, "*Kolla* es un proyecto oficial de *OpenStack* para crear contenedores *Docker* listos para producción para los servicios de *OpenStack*" (Vainio, A., 2020), lo que respalda su relevancia y solidez como tecnología para gestionar imágenes de contenedores en entornos complejos. El uso de Docker permite a *Kolla-Ansible* una arquitectura modular, ya que cada servicio principal de *OpenStack* se ejecuta como un contenedor independiente, lo que permite instalar, reiniciar o actualizar cada componente sin afectar al resto del clúster.

Además, el elevado nivel de automatización que ofrece permite reducir considerablemente el tiempo necesario para un despliegue completo: mientras que una instalación manual de *OpenStack* puede requerir entre 40 y 60 horas-hombre, debido a la configuración detallada de numerosas dependencias y servicios, la implementación con *Kolla-Ansible* reduce este tiempo a un rango estimado de 8 a 12 horas, incluyendo validaciones y pruebas. Esta eficiencia se alcanza gracias a tareas automatizadas por Ansible, que permiten desplegar múltiples contenedores de forma simultánea.

Asimismo, la escalabilidad que proporciona facilita la expansión horizontal del clúster, ya que la incorporación de nodos de cómputo o control se realiza mediante simples actualizaciones del archivo de inventario y la ejecución de comandos específicos de *Ansible*, sin necesidad de reinstalar todo el entorno.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 65 - 80

2.4 OPENSTACK-ANSIBLE

OpenStack-Ansible es una herramienta de implementación de *OpenStack* basado en *Ansible*. A diferencia de usar *Docker*, puede ejecutarse en contenedores basados en LXC o instalarse directamente en hardware físico (*bare-metal*). Es una solución adaptable y poderosa, ideal para entornos complejos que requieren un control detallado sobre la infraestructura.

Sin embargo, como señala Vainio, "es un método de implementación de bajo nivel y requiere un buen entendimiento del entorno objetivo y de *Ansible*" (Vainio, A., 2020), lo cual puede ser un obstáculo para los administradores menos experimentados. Aunque tiene una curva de aprendizaje compleja, su énfasis en configuraciones muy personalizables lo hace adecuado para necesidades más especializadas.

2.5 DEVSTACK

DevStack es una herramienta específicamente diseñada para implementaciones en entornos de desarrollo, pruebas y formación técnica. Permite poner en funcionamiento una instancia de *OpenStack* de manera rápida y sencilla, lo que la convierte en una opción ideal para la experimentación, el aprendizaje y el prototipado en escenarios controlados. Sin embargo, no debe considerarse una alternativa viable para entornos de producción, ya que no ofrece robustez, alta disponibilidad ni soporte para configuraciones avanzadas y escalables. Su arquitectura está orientada a instalaciones temporales de un solo nodo, sin los mecanismos necesarios para garantizar continuidad operativa.

2.6 TRIPLEO

OpenStack se utiliza como herramienta de implementación para desplegar *OpenStack* en sí mismo, esto se conoce como TripleO (*OpenStack* Sobre *OpenStack*), una solución integrada. Es una opción útil en entornos de producción más grandes y despliegues complejos, pero la configuración puede llevar bastante tiempo. TripleO es un instalador que, de manera única, permite gestionar infraestructuras escalables y altamente disponibles.

2.7 DESPLIEGUE MANUAL

En el despliegue manual, se debe instalar y configurar cada servicio de *OpenStack* individualmente. Se obtiene control total, pero es lento y propenso a errores, por lo que sólo debe usarse donde se necesite una configuración extremadamente personalizada o donde otras herramientas no funcionen.

A continuación, en la Tabla 1, se presenta una comparativa que muestra las principales diferencias entre las herramientas y el despliegue manual basándose en los criterios analizados, con el fin de facilitar la comprensión de las diferencias entre los distintos despliegues de *OpenStack*.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 66 - 80

Tabla 1

Comparativa técnica de despliegue en OpenStack: automático y manual

Herramienta	Enfoque	Ventajas	Desventajas	Casos de Uso
Kolla-Ansible	Contenedores *Docker* + *Ansible*	Modularidad y escalabilidad Configuración predefinida Fácil integración con Ansible Reducción de conflictos entre dependencias	Requiere conocimientos previos en *Docker* y *Ansible*	Entornos de producción que requieren eficiencia, automatización y facilidad de mantenimiento
OpenStack-Ansible	Contenedores LXC + *Ansible*, Hardware + *Ansible*	Gran flexibilidad Automatización robusta	Gran complejidad Curva de aprendizaje pronunciada	Entornos de producción, desarrollo y pruebas
DevStack	Instalación ligera para desarrollo y pruebas	Rápida implementación Simplicidad para experimentar con OpenStack	No apto para producción Falta de robustez y soporte	Sólo utilizado para pruebas
TripleO	*OpenStack* sobre *OpenStack*	Infraestructura escalable Alta Disponibilidad Solución integrada	Configuración inicial compleja Complejidad operativa	Grandes entornos de producción con alta demanda de escalabilidad
Despliegue manual	Instalación manual de componentes	Control total sobre cada componente	Proceso lento y propenso a errores Altos costos de mantenimiento Demanda de experiencia	Casos de ajuste extremadamente personalizado o donde otras herramientas no sean viables

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 67 - 80

3. RESULTADOS

La elección de la forma de instalación depende directamente de las necesidades particulares de cada infraestructura. En el caso del Centro de Datos de la DGTIC, el enfoque está en implementar una nube privada que priorice flexibilidad, escalabilidad y automatización.

En este escenario, *Kolla-Ansible* destaca al ofrecer una instalación modular y eficiente en contenedores que utiliza significativamente menos tiempo para completarse que las implementaciones manuales de *OpenStack*; esta herramienta ofrece un punto óptimo entre la sobrecarga operativa y la sobrecarga de mantenimiento gracias a su uso de tecnologías de contenedores. Por el contrario, TripleO tiene una arquitectura para gestionar *OpenStack* más compleja y genera exceso operativo, mientras que *Kolla-Ansible* se beneficia de la simplicidad de usar *Docker* y minimiza los conflictos de dependencias a través de su uso de contenedores ligeros.

Por su parte, *OpenStack-Ansible* proporciona un buen nivel de automatización, actuando como una solución intermedia, aunque requiere dominar bastante *Ansible*, sumando una curva de aprendizaje compleja para el administrador. *DevStack*, por otro lado, está diseñado principalmente para entornos de desarrollo, lo que, si bien permite implementaciones rápidas, lo hace menos viable para operar en un entorno de producción debido a lo provisional que es y la falta de adaptabilidad para dichos entornos. Finalmente, la implementación manual permite el control completo de los servicios; la cantidad de esfuerzo técnico, tiempo y los costos de mantenimiento involucrados la hacen impráctica para implementar en producción.

Para evaluar si *Kolla-Ansible* cumple con los requerimientos como herramienta de implementación, se realizó la instalación de un entorno *OpenStack* compuesto por cinco nodos. Dos nodos se asignaron a tareas de control y los tres restantes se dispusieron para cómputo. Toda la información sobre el proceso de instalación, incluidas las etapas realizadas y configuraciones aplicadas, se encuentra documentada en los anexos para su consulta.

La implementación con *Kolla-Ansible* permitió automatizar eficientemente procesos complejos, como la configuración de nodos, generación de contraseñas seguras, creación de certificados TLS y el despliegue completo de servicios. Este enfoque no sólo simplificó el proceso al reducir drásticamente la intervención manual, sino que disminuyó significativamente los riesgos de errores humanos y proporcionó un ambiente más estable y funcional.

La configuración ofrecida por *Kolla-Ansible* está diseñada para garantizar tanto la operatividad actual como una expansión futura sin inconvenientes. Su arquitectura modular facilita la integración de nuevos nodos en el clúster, ya sean de control o cómputo, sin interrumpir el rendimiento del sistema existente. Además, esta estructura simplifica el crecimiento de la infraestructura mientras asegura un balance dinámico de la carga, y maximiza el uso eficiente de recursos en beneficio del rendimiento global del clúster.

4. CONCLUSIÓN

En general la implementación de *OpenStack* mediante *Kolla-Ansible* representa un avance significativo en la estandarización y automatización de los componentes que integran una infraestructura en la nube.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 68 - 80

Este enfoque conduce no sólo a grandes ventajas técnicas (optimización de procesos, mayor gestión de entornos complejos), sino que también refleja la simplificación de operaciones y hace más accesibles tecnologías que eran consideradas complejas.

Además, el hecho de considerar a *Kolla-Ansible* como una opción para una futura implementación permitiría al Centro de Datos mantener un control total sobre la infraestructura, lo que contribuiría no sólo a una reducción significativa de los costos operativos y, en consecuencia, a un ahorro importante para la Universidad, sino también a fortalecer la autonomía técnica del Centro de Datos para gestionar y escalar su nube privada de forma independiente.

No obstante, como todas las soluciones tecnológicas avanzadas, su potencial total sólo se logra cuando se comprende a fondo tanto en teoría como en práctica. Sabemos que alcanzar buenos resultados requiere también una ejecución cuidadosa, diseñada para ajustarse a las características particulares y las demandas específicas de cada entorno de aplicación. Por esta razón, es fundamental llevar a cabo un análisis profundo y contar con un conocimiento sólido que permita guiar este proceso de manera efectiva.

A diferencia de los métodos tradicionales, que suelen ser más rígidos y estructurados, *Kolla-Ansible* se presenta como algo más que un conjunto de herramientas o guías. Este proyecto propone una forma de trabajo innovadora que busca cambiar la manera en que se gestiona la infraestructura en la nube. En un contexto donde la flexibilidad y la eficiencia son esenciales, *Kolla-Ansible* desafía las prácticas convencionales al ofrecer un enfoque que podría transformar la forma en que se diseñan y operan las plataformas, al promover el uso de contenedores como una solución clave.

REFERENCIAS

Bravo Roldán, L.A. (2022). *Implementación de la arquitectura de cloud computing OpenStack para el despliegue y disponibilidad de aplicaciones en la empresa DICONST* [Tesis de maestría, Universidad Tecnológica del Perú]). Repositorio Institucional UTP. https://hdl.handle.net/20.500.12867/6911

OpenStack Foundation. (2019). *Kolla-Ansible Documentation: Stein Release*. Recuperado el 2 de abril de 2025 de https://docs.openstack.org/kolla-ansible/stein/

Tatta Vishwa Mithra, & Gudipati Sai Vivek. (2022). *Investigation of an automatic deployment transformation method for OpenStack* [Tesis de maestría en Ingeniería Eléctrica con énfasis en Sistemas de Telecomunicaciones, Blekinge Institute of Technology]. DiVA Portal. https://www.diva-portal.org/smash/get/diva2:1674200/FULLTEXT02

Vainio, A. (2020). *Automated Software Configuration for Cloud Deployment* [Master's thesis, University of Helsinki]. Helda. https://helda.helsinki.fi/server/api/core/bitstreams/793f47f6-6cf6-47b6-a6be-7d2903550a7e/content

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 69 - 80

ANEXO A

Instalación de nube privada *OpenStack* con herramienta de despliegue *kolla-ansible*

La implementación de *OpenStack* utilizando *Kolla-Ansible* se posiciona como una alternativa estratégica para establecer una nube privada que sea robusta y escalable.

Esta solución emplea contenedores *Docker* para ejecutar los servicios de *OpenStack*, lo que simplifica tanto el proceso de implementación como el mantenimiento. Además, esta metodología proporciona un enfoque ágil y moderno para gestionar actualizaciones y el ciclo de vida de los servicios dentro de la infraestructura.

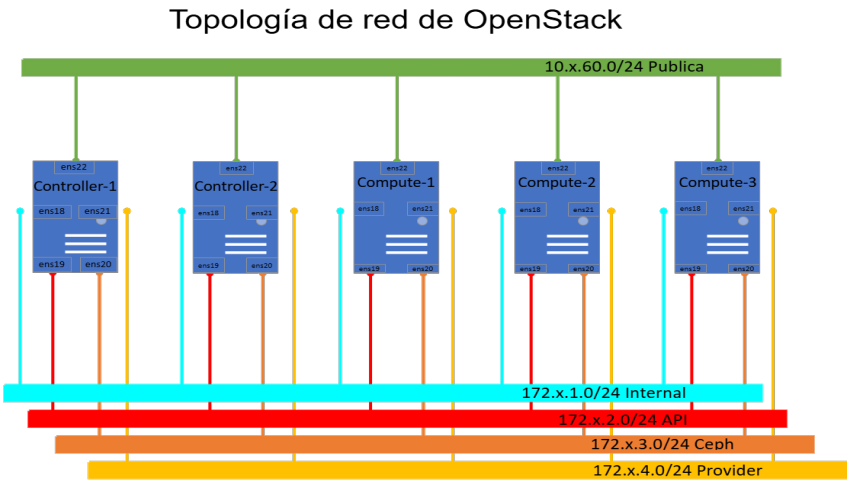
La base de este proyecto está centrada en un entorno virtualizado que funciona con Proxmox, donde se configuraron 5 máquinas virtuales dedicadas a nodos de control (2 *controller*) y nodos de cómputo (3 *compute*).

En el aspecto de red se definieron 5 redes. Red *Ceph* permitirá la comunicación entre nodos para la creación del almacenamiento de *Ceph*, la red Internal sirve para la comunicación entre los *backend* de los servicios de *OpenStack*, la red Pública es utilizado por los servicios de *OpenStack* para proporcionar acceso externo y garantizar alta disponibilidad mediante un mecanismo de *failover*, la red API se emplea por los servicios de *OpenStack* para sus APIs públicas, internas y de administración, y la red *Provider* es la que manejará el tráfico de red externo en el servicio de *Neutron*. Un esquema de cómo será la topología de red se muestra en la Figura 1, las direcciones IP incluyen una "x" para indicar que se utilizan únicamente como ejemplo.

Este enfoque basado en la virtualización ofrece una solución versátil que se adapta con facilidad a los requerimientos futuros. Al seguir el procedimiento detallado, se podrá implementar un sistema *OpenStack* de manera efectiva.

Figura 1

Topología del clúster para implementación de OpenStack



https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 70 - 80

Requisitos de Hardware

Para esta implementación, se utilizarán los siguientes requisitos para la creación de las máquinas virtuales:

Nodo	CPU	RAM	Almacenamiento	Almacenamiento	Almacenamiento	Red
Controller-1	4 núcleos	16 GB	50 GB	40 GB	40 GB	1 Gbps
Controller-2	4 núcleos	16 GB	50 GB	40 GB	40 GB	1 Gbps
Compute-1	4 núcleos	16 GB	50 GB	40 GB	40 GB	1 Gbps
Compute-2	4 núcleos	16 GB	50 GB	40 GB	40 GB	1 Gbps
Compute-3	4 núcleos	16 GB	50 GB	40 GB	40 GB	1 Gbps

1. INSTALACIÓN Y CONFIGURACIÓN DE HERRAMIENTAS Y DEPENDENCIAS

1.1 AGREGAR SERVIDORES AL ARCHIVO /ETC/HOSTS EN EL NODO DEPLOYER (CONTROLLER1)

El archivo /etc/hosts se utiliza para mapear direcciones IP a nombres de host dentro de la red local. Al agregar estos registros, se podrá identificar y comunicarse con los distintos nodos dentro del clúster *OpenStack*.

Editar /etc/hosts con la siguiente información:

```
### Lista de servidores
172.x.3.21 controller-1
172.x.3.22 controller-2
172.x.3.24 compute-1
172.x.3.25 compute-2
172.x.3.26 compute-3
```

1.2 CONFIGURACIÓN DE LA CLAVE SSH PARA EL USUARIO ROOT EN LOS NODOS

El uso de la clave SSH permite una autenticación segura sin necesidad de contraseñas, lo que facilita la comunicación entre los nodos.

Comandos:

Generar la clave SSH:

```
# ssh-keygen -t rsa
```

Copiar la clave pública a cada nodo:

```
# ssh-copy-id root@controller-1
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 71 - 80

```
# ssh-copy-id root@controller-2
# ssh-copy-id root@compute-1
# ssh-copy-id root@compute-2
# ssh-copy-id root@compute-3
```

1.3 CONFIGURACIÓN DEL NOMBRE DE HOST Y ZONA HORARIA EN TODOS LOS NODOS

Es crucial que todos los nodos tengan configurados nombres de host coherentes y la misma zona horaria para garantizar la consistencia en las operaciones del clúster.

Comandos:

```
for node in controller-{1..2} compute-{1..3}
do
  echo "--- $node ---"
  ssh root@$node hostnamectl set-hostname $node
  ssh root@$node timedatectl set-timezone America/Mexico_City
  echo ""
  sleep 2
done
```

1.4 INSTALACIÓN DE DOCKER CE EN CADA NODO

Docker se usa para facilitar la implementación de servicios y componentes en los nodos.

Comandos:

```
# apt-get install apt-transport-https \
   ca-certificates \
   curl \
   gnupg-agent \
   software-properties-common -y
#  curl  -fsSL  https://download.docker.com/linux/ubuntu/gpg  |  sudo  gpg
--dearmor > /etc/apt/trusted.gpg.d/docker-ce.gpg
# echo "deb [arch=amd64] https://download.docker.com/linux/ubuntu $(lsb_
release -sc) stable" > /etc/apt/sources.list.d/docker-ce.list
# apt-get update; apt-get install docker-ce docker-ce-cli containerd.io -y
# systemctl enable --now Docker
```

2. INSTALACIÓN DE OPENSTACK CON KOLLA-ANSIBLE

2.1 AGREGAR SERVIDORES AL ARCHIVO /ETC/HOSTS EN CONTROLLER-1

El archivo /etc/hosts se utiliza para mapear direcciones IP a nombres de host en la red local. Al agregar estos registros, *Kolla-Ansible* podrá identificar y comunicarse con los distintos nodos dentro del clúster.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 72 - 80

Editar /etc/hosts con la siguiente información:

```
172.x.1.21 controller-1 controller-1.internal.unam.mx
172.x.1.22 controller-2 controller-2.internal.unam.mx
172.x.1.24 compute-1 compute-1.internal.unam.mx
172.x.1.25 compute-2 compute-2.internal.unam.mx
172.x.1.26 compute-3 compute-3.internal.unam.mx
172.x.1.55 internal.unam.mx

10.x.60.21 controller-1.public.unam.mx
10.x.60.22 controller-2.public.unam.mx
10.x.60.24 compute-1.public.unam.mx
10.x.60.25 compute-2.public.unam.mx
10.x.60.26 compute-3.public.unam.mx
10.x.60.55 public.unam.mx
```

2.2 CONFIGURAR CLUSTER CEPH

Instalar y configurar un Clúster *Ceph* con Cephadm, se incorpora desde la instalación inicial en el nodo *deployer* (hosts y nodos), hasta el despliegue de OSDs para gestionar el almacenamiento de *Openstack*.

2.2.1 CREAR UN POOL PARA OPENSTACK

Comando:

```
# ceph osd pool create volumes
# ceph osd pool set volumes size 3
# rbd pool init volumes
# ceph osd pool create images
# ceph osd pool set images size 3
# rbd pool init images
# ceph osd pool create backups
# ceph osd pool set backups size 3
# rbd pool init backups
# ceph osd pool create vms
# ceph osd pool set vms size 3
# rbd pool init vms
```

2.2.2 CREAR CEPH KEYRING

```
# ceph auth get-or-create client.glance mon 'allow r' osd 'allow class-read object_prefix rbd_children, allow rwx pool=images' -o /etc/ceph/ceph.client.glance.keyring

# ceph auth get-or-create client.cinder mon 'allow r' osd 'allow class-read object_prefix rbd_children, allow rwx pool=volumes, allow rwx pool=images' -o /etc/ceph/ceph.client.cinder.keyring
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 73 - 80

```
# ceph auth get-or-create client.nova mon 'allow r' osd 'allow class-
read object_prefix rbd_children, allow rwx pool=vms, allow rx pool=ima-
ges' -o /etc/ceph/ceph.client.nova.keyring
# ceph auth get-or-create client.cinder-backup mon 'allow r' osd 'allow
class-read object_prefix rbd_children, allow rwx pool=backups' -o /etc/
ceph/ceph.client.cinder-backup.keyring
```

2.2.3 ACTUALIZACIÓN DEL SISTEMA Y CREACIÓN DEL ENTORNO VIRTUAL

El sistema debe estar actualizado para asegurar que se cuente con las últimas versiones de paquetes y dependencias necesarias para la instalación.

Comandos:

```
# apt-get update -y

# apt-get install python3-dev libffi-dev gcc libssl-dev python3-selinux
python3-setuptools python3-venv -y
```

2.2.4 ACTIVACIÓN DEL ENTORNO VIRTUAL

Es fundamental crear un entorno virtual en Python para aislar las dependencias específicas de *Kolla-Ansible* y *OpenStack*.

Comandos:

```
# python3 -m venv kolla-venv
# echo "source ~/kolla-venv/bin/activate" >> ~/.bashrc
# source ~/kolla-venv/bin/actívate
```

2.2.5 INSTALACIÓN DE ANSIBLE Y KOLLA-ANSIBLE

Kolla-Ansible depende de *Ansible* para automatizar la instalación y configuración de *OpenStack*. Debemos instalar las versiones adecuadas de estas herramientas.

Comandos:

```
# pip install -U pip
# pip install 'ansible-core>=2.14,<2.16'
# ansible --version
# pip install git+https://opendev.org/openstack/kolla-ansible@master
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 74 - 80

2.3 CONFIGURACIÓN DE INVENTARIO DE MÚLTIPLES NODOS

2.3.1 MODIFICACIÓN DEL ARCHIVO DE INVENTARIO MULTINODE

El archivo *multinode* define los nodos y sus roles dentro del clúster de *OpenStack*. Se debe comprobar que todos los nodos estén correctamente definidos.

Comandos:

```
# cp multinode multinode.bak
# nano multinode
```

Contenido de *multinode*:

```
[control]
controller-1.internal.unam.mx ansible_host=172.x.1.21
controller-2.internal.unam.mx ansible_host=172.x.1.22

[network]
controller-1.internal.unam.mx
controller-2.internal.unam.mx

[compute]
controller-1.internal.unam.mx
controller-2.internal.unam.mx
compute-1.internal.unam.mx ansible_host=172.x.1.24
compute-2.internal.unam.mx ansible_host=172.x.1.25
compute-3.internal.unam.mx ansible_host=172.x.1.26

[monitoring]
controller-1.internal.unam.mx
controller-2.internal.unam.mx

[storage]
controller-1.internal.unam.mx
controller-2.internal.unam.mx
compute-1.internal.unam.mx
compute-2.internal.unam.mx
compute-3.internal.unam.mx

[deployment]
localhost       ansible_connection=local
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 75 - 80

2.3.2 VERIFICACIÓN DE CONEXIÓN CON ANSIBLE

Es importante verificar que los nodos sean accesibles mediante *Ansible* antes de proceder con la implementación.

Comando:

```
# ansible -i multinode all -m ping
```

2.4 GENERACIÓN DE CONTRASEÑAS Y CERTIFICADOS TLS

2.4.1 GENERACIÓN DE CONTRASEÑAS

Para garantizar la seguridad de los servicios de *OpenStack*, es necesario generar contraseñas aleatorias para cada uno de los servicios.

Comando:

```
# kolla-genpwd
```

2.4.2 GENERACIÓN DE CERTIFICADOS TLS

Es importante generar los certificados TLS para garantizar las comunicaciones seguras entre los nodos de *OpenStack*.

Comando:

```
# kolla-ansible certificates -i multinode
```

2.4.3 GENERACIÓN DE CLAVE PRIVADA

Es importante generar una clave privada para generar posteriormente un certificado autofirmado.

Comando:

```
# openssl genpkey -algorithm RSA -out /etc/ssl/private/private.key -aes256
```

2.4.4 GENERAR UN CERTIFICADO AUTOFIRMADO

Este tipo de certificado es útil para configurar el *HAProxy* que permite el direccionamiento de los servicios de *OpenStack*

Comando:

```
# openssl req -new -x509 -key /etc/ssl/private/private.key -out /etc/ssl/
private/haproxy-public.pem -days 365
# openssl req -new -x509 -key /etc/ssl/private/private.key -out /etc/ssl/
private/haproxy-internal.pem -days 365
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 76 - 80

2.5 REACIÓN DE DIRECTORIOS DE CONFIGURACIÓN DE KOLLA-ANSIBLE

Kolla-Ansible necesita directorios específicos para almacenar las configuraciones de los servicios de *OpenStack* como Nova, *Glance* y *Cinder*.

Comandos:

```
# mkdir -p /etc/kolla/config
# mkdir -p /etc/kolla/config/nova
# mkdir -p /etc/kolla/config/glance
# mkdir -p /etc/kolla/config/cinder/cinder-volume
# mkdir -p /etc/kolla/config/cinder/cinder-backup
# cp /etc/ceph/ceph.conf /etc/kolla/config/cinder/
# cp /etc/ceph/ceph.conf /etc/kolla/config/nova/
# cp /etc/ceph/ceph.conf /etc/kolla/config/glance/
# cp /etc/ceph/ceph.client.glance.keyring /etc/kolla/config/glance/
# cp /etc/ceph/ceph.client.nova.keyring /etc/kolla/config/nova/
# cp /etc/ceph/ceph.client.cinder.keyring /etc/kolla/config/nova/
# cp /etc/ceph/ceph.client.cinder.keyring /etc/kolla/config/cinder/cin-
der-volume/
# cp /etc/ceph/ceph.client.cinder.keyring /etc/kolla/config/cinder/cin-
der-backup/
# cp /etc/ceph/ceph.client.cinder-backup.keyring /etc/kolla/config/cin-
der/cinder-backup/

for node in controller-{2} compute-{1..3}
do
  scp -r /etc/ceph/ root@$node:/etc/
done
```

2.6 EDICIÓN DEL ARCHIVO GLOBALS.YML

El archivo globals.yml es el archivo central para la configuración de *Kolla-Ansible* y define parámetros clave como el uso de TLS, la distribución base y las direcciones IP.

Comando:

```
nano /etc/kolla/globals.yml
```

Configuraciones relevantes:

```
---
workaround_ansible_issue_8743: yes
kolla_base_distro: "ubuntu"
openstack_release: "master"
kolla_internal_vip_address: "172.x.2.55"
kolla_internal_fqdn: "internal.unam.mx"
kolla_external_vip_address: "10.x.60.55"
kolla_external_fqdn: "public.unam.mx"
kolla_external_vip_interface: "ens22"
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 77 - 80

```
api_interface: "ens19"
tunnel_interface: "ens20"
neutron_external_interface: "ens21"
neutron_plugin_agent: "ovn"
kolla_enable_tls_internal: "yes"
kolla_enable_tls_external: "yes"
kolla_copy_ca_into_containers: "yes"
kolla_external_fqdn_cert: "/etc/ssl/private/haproxy-public.pem"
kolla_external_fqdn_key: "/etc/ssl/private/haproxy-public.pem"
kolla_internal_fqdn_cert: "/etc/ssl/private/haproxy-internal.pem"
kolla_internal_fqdn_key: "/etc/ssl/private/haproxy-internal.pem"
openstack_cacert: "/etc/ssl/certs/ca-certificates.crt"
kolla_enable_tls_backend: yes
enable_openstack_core: "yes"
enable_cinder: "yes"
enable_fluentd: "yes"
enable_neutron_provider_networks: "yes"
cinder_cluster_name: "cinder-cluster"
ceph_glance_user: "glance"
ceph_glance_keyring: "client.glance.keyring"
ceph_glance_pool_name: "images"
ceph_cinder_user: "cinder"
ceph_cinder_keyring: "client.cinder.keyring"
ceph_cinder_pool_name: "volumes"
ceph_cinder_backup_user: "cinder-backup"
ceph_cinder_backup_keyring: "client.cinder-backup.keyring"
ceph_cinder_backup_pool_name: "backups"
ceph_nova_user: "nova"
ceph_nova_keyring: "client.nova.keyring"
ceph_nova_pool_name: "vms"
glance_backend_ceph: "yes"
cinder_backend_ceph: "yes"
nova_backend_ceph: "yes"
nova_compute_virt_type: "kvm"
neutron_ovn_distributed_fip: "yes"
```

2.7 FASE DE IMPLEMENTACIÓN DE OPENSTACK

2.7.1 CONFIGURACIÓN INICIAL DE LOS SERVIDORES

Es necesario configurar los servidores antes de la instalación de *OpenStack*.

Comando:

```
# kolla-ansible bootstrap-servers -i multinode
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 78 - 80

2.7.2 VERIFICACIÓN PREVIA Y DESPLIEGUE

Antes de desplegar *OpenStack*, se deben realizar verificaciones para asegurar que todo esté en orden.

Comandos:

```
# kolla-ansible prechecks -i multinode
# kolla-ansible deploy -i multinode
```

2.7.3 POST-DESPLIEGUE

Una vez que *OpenStack* está desplegado, se deben realizar pasos adicionales.

Comando:

```
# kolla-ansible post-deploy -i multinode
```

2.8 CONFIGURACIÓN DEL CLIENTE OPENSTACK

2.8.1 INSTALACIÓN DEL CLIENTE OPENSTACK

Para interactuar con *OpenStack* desde la línea de comandos, es necesario instalar el cliente *OpenStack*.

Comandos:

```
# cat /etc/kolla/certificates/ca/root.crt | sudo tee -a /etc/ssl/certs/
ca-certificates.crt
# pip3 install python-openstackclient
```

2.8.2 VERIFICACIÓN DEL CLIENTE

Verifica la instalación del cliente de *OpenStack*.

Comando:

```
# openstack –versión
```

2.8.3 VERIFICACIÓN DEL CLÚSTER DE OPENSTACK

Verificación de los servicios en ejecución para el funcionamiento del clúster de *OpenStack*.

```
# openstack endpoint list
# openstack service list
# openstack compute service list;
# openstack network agent list
# openstack volume service list
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 79 - 80

2.9 AGREGAR NODOS ADICIONALES

2.9.1 AGREGAR LA IP Y NOMBRE DEL HOST AL INVENTARIO

En el archivo *multinode* define el nodo nuevo y sus roles dentro del clúster de *OpenStack*. Para consultar los detalles del archivo *multinode*, se recomienda consultar la sección 3.5.1 del Manual de instalación de *OpenStack*, utilizando *Kolla-Ansible*. Para el ejemplo, el nodo se nombrará controller-3.internal.unam.mx

Comandos:

```
# cp multinode multinode.bak
# nano multinode
```

Contenido de multinode:

```
[control]
controller-1.internal.unam.mx ansible_host=172.x.1.21
controller-2.internal.unam.mx ansible_host=172.x.1.22
controller-3.internal.unam.mx ansible_host=172.x.1.23

[network]
controller-1.internal.unam.mx
controller-2.internal.unam.mx
controller-3.internal.unam.mx

[compute]
controller-1.internal.unam.mx
controller-2.internal.unam.mx
controller-3.internal.unam.mx
compute-1.internal.unam.mx ansible_host=172.x.1.24
compute-2.internal.unam.mx ansible_host=172.x.1.25
compute-3.internal.unam.mx ansible_host=172.x.1.26

[monitoring]
controller-1.internal.unam.mx
controller-2.internal.unam.mx
controller-3.internal.unam.mx

[storage]
controller-1.internal.unam.mx
controller-2.internal.unam.mx
controller-3.internal.unam.mx
compute-1.internal.unam.mx
compute-2.internal.unam.mx
compute-3.internal.unam.mx

[deployment]
localhost       ansible_connection=local
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.117 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 80 - 80

2.9.2 VERIFICACIÓN DE CONEXIÓN CON ANSIBLE

Comando:

```
# ansible -i multinode controller-3.internal.unam.mx -m ping
```

2.9.3 CONFIGURACIÓN INICIAL DE LOS SERVIDORES

Es necesario configurar los servidores antes de la instalación de *OpenStack*, colocando las dependencias necesarias.

Comando:

```
# kolla-ansible bootstrap-servers -i multinode --limit controller-3.in-
ternal.unam.mx
```

2.9.4 DESCARGAR LAS IMÁGENES DE CONTENEDORES

Se descargan las imágenes de contenedores necesarias para el nodo *controller* con el siguiente comando:

Comando:

```
# kolla-ansible pull -i multinode --limit controller-3.internal.unam.mx
```

2.9.5 DESPLIEGUE DE OPENSTACK EN EL NODO CONTROLLER-3

Comando:

```
# kolla-ansible deploy -i multinode --limit control
```

2.9.6 VERIFICACIÓN DE NODO AGREGADO

Comando:

```
# openstack host list
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121

Vol. 3, Núm. 3. julio-septiembre 2025, págs. 81 - 90

Implementación de Nessus para el análisis de vulnerabilidades en un centro de datos

Información del reporte:

Para citar este reporte técnico:

Pérez Santillán, P. T. (2025). Implementación de Nessus para el análisis de vulnerabilidades en un centro de datos. *Cuadernos Técnicos Universitarios de la DGTIC, 3* (3) páginass(81 - 90).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121

Pedro Temachti Pérez Santillán

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Universidad Nacional Autónoma de México

ptsantillan@unam.mx

ORCID: 0009-0000-2626-9073

Resumen

El Centro de Datos de una universidad alberga información vital y sensible, por lo que la identificación y corrección de vulnerabilidades en su infraestructura digital es crucial. La creciente complejidad de las infraestructuras digitales, especialmente con la adopción de tecnologías de virtualización y servicios en la nube, introdujo nuevos desafíos de seguridad, lo que hace indispensable la gestión de vulnerabilidades. Ante la gran cantidad de servidores virtuales y la diversidad de sistemas operativos en ellos, la revisión manual de seguridad ya no es viable, lo que motivó la necesidad de implementar herramientas de automatización para el análisis de vulnerabilidades. Se decidió implementar y evaluar la herramienta Nessus en un entorno de pruebas, con el objetivo de identificar y reportar posibles brechas de seguridad en la infraestructura virtualizada del Centro de Datos de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). La elección de Nessus se fundamentó en su amplio reconocimiento en la industria, así como su uso de manera exitosa en otras instituciones académicas para la detección proactiva y automatizada de vulnerabilidades.

La metodología consistió en instalar Nessus en una máquina virtual, dentro de un clúster de pruebas con el hipervisor Proxmox y diversas máquinas virtuales con algunas brechas de seguridad. Para las direcciones IP objetivo, se realizaron escaneos básicos y con credenciales,

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 82 - 90

y se emplearon los rangos de puertos predeterminados. Los resultados del análisis proporcionaron un número total de vulnerabilidades identificadas y su distribución por nivel de gravedad, lo que permitió realizar recomendaciones específicas para mejorar la seguridad del entorno de pruebas. El análisis demostró la eficiencia de Nessus para identificar y clasificar vulnerabilidades en infraestructuras virtualizadas complejas, en las que múltiples recursos físicos como servidores, almacenamiento y redes han sido virtualizados, resaltando la importancia de un programa continuo de gestión de vulnerabilidades y la adopción de mejores prácticas de seguridad para mejorar la capacidad de la infraestructura digital, con el fin de resistir y recuperarse de incidentes.

Palabras clave:

Nessus, vulnerabilidades, centro de datos, máquina virtual, virtualización, seguridad, ciberseguridad.

Abstract

A university's data center hosts vital and sensitive information, making identification and correction of vulnerabilities in its digital infrastructure crucial. The increasing complexity of digital infrastructures, especially with the adoption of virtualization technologies and cloud services, has introduced new security challenges, making vulnerability management essential. Given the large number of virtual servers and the diversity of operating systems within them, manual security reviews are no longer viable, which motivated the need to implement automated tools for vulnerability analysis. It was decided to implement and evaluate the Nessus tool in a testing environment to identify and report potential security breaches in the virtualized infrastructure of the Data Center of the Directorate General of Computing and Information and Communication Technologies (DGTIC). The choice of Nessus was based on its broad recognition in the industry, as well as its successful use in other academic institutions for proactive and automated vulnerability detection.

The methodology consisted of installing Nessus on a virtual machine within a test cluster running the Proxmox hypervisor and several virtual machines with some security breaches. For the target IP addresses, basic and credentialed scans were performed, and default port ranges were used. The analysis results provided a total number of identified vulnerabilities and their distribution by severity level, allowing for specific recommendations to improve the security of the test environment. The analysis demonstrated Nessus's effectiveness in identifying and classifying vulnerabilities in complex virtualized infrastructures, where multiple physical resources such as servers, storage, and networks have been virtualized. This highlights the importance of an ongoing vulnerability management program and the adoption of security best practices to improve the digital infrastructure's ability to withstand and recover from incidents.

Keywords:

Nessus, vulnerabilities, data center, virtual machine, virtualization, security, cybersecurity.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 83 - 90

1. INTRODUCCIÓN

El Centro de Datos tiene servidores de almacenamiento digitales que albergan una gran cantidad de datos sensibles para el desarrollo de las actividades académicas y administrativas de la Universidad. La identificación y la remediación de vulnerabilidades de esta infraestructura digital es esencial para asegurar los servicios digitales que se ofrecen.

La evolución de las infraestructuras digitales de un Centro de Datos ha llevado a un aumento considerable en su complejidad. La adopción de tecnologías de virtualización, si bien ofrece beneficios en términos de optimización de recursos y flexibilidad, también introduce nuevos desafíos de seguridad. La gestión de la seguridad, en entornos con múltiples hipervisores, requiere conocimientos especializados de cada una de las herramientas utilizadas. Existen estudios que abordan la optimización del rendimiento de la virtualización y explican que múltiples niveles de hipervisores pueden complicar la gestión de la seguridad (Lim, J. y Nieh, J., 2020).

La gestión de vulnerabilidades, entendida como el proceso de identificar, clasificar, remediar y mitigar las debilidades de seguridad, se vuelve fundamental para mantener la integridad de estos entornos complejos. Es necesario adoptar estrategias proactivas, por ejemplo, utilizar herramientas de escaneo automatizado en la detección de fallos de seguridad susceptibles de ser explotados por agentes maliciosos (Elastic. s.f.).

No obstante, la tarea de garantizar la seguridad se vuelve particularmente compleja cuando se trata de infraestructuras tecnológicas de gran tamaño. El caso del Centro de Datos de la DGTIC, que aloja a más de mil servidores virtuales que se ejecutan sobre múltiples hipervisores, presenta un desafío significativo para la realización de revisiones de seguridad de manera manual. La magnitud de esta infraestructura hace inviable la inspección individual de cada servidor, tanto por la cantidad de tiempo y recursos que demandaría como por la dificultad de mantener una visión coherente y actualizada del estado de seguridad. La diversidad de sistemas operativos con los que se entregan los servidores virtuales añade una capa adicional de complejidad, ya que cada sistema operativo puede tener sus propias vulnerabilidades y requerir tanto herramientas como conocimientos específicos para su análisis. Ante esta situación, la necesidad de implementar soluciones de automatización para el análisis de vulnerabilidades se hizo indispensable.

El presente reporte técnico describe el proceso de implementación de la herramienta Nessus en un entorno de pruebas y un análisis de los resultados obtenidos al emplearla como analizador de vulnerabilidades en un clúster de servidores del Centro de Datos, con el objetivo de evaluar su capacidad para identificar y reportar las vulnerabilidades de seguridad presentes en la infraestructura virtualizada, realizado en el segundo semestre de 2024.

2. DESARROLLO TÉCNICO

Elección de la herramienta

Existen investigaciones sobre la implementación de Nessus en redes de campus universitarios, en las que se destaca su eficacia en la identificación de vulnerabilidades (Railkar, D., 2022). Esto brinda un precedente para elegir la herramienta y sugiere que Nessus se ha implementado con éxito en otras

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 84 - 90

universidades (Chhillar, K., 2021). Entre ellas, la Universidad de Harvard emplea Nessus para realizar pruebas de vulnerabilidad proactivas y automatizadas en sus instancias de servidores; lo integran con sistemas de gestión de tickets para dar seguimiento a los riesgos detectados y su remediación (Harvard University Information Technology Security Operations, 2024).

Otras universidades de Estados Unidos incluyen la herramienta como parte de sus procedimientos de seguridad. Por ejemplo, la Universidad de Texas en Austin (2021) utiliza Nessus para realizar escaneos de vulnerabilidades en sus sistemas. La Universidad de California en Berkeley (2025), por medio de su Oficina de Seguridad, realiza escaneos de vulnerabilidades utilizando Nessus.

Estos casos sugieren que Nessus es una herramienta considerada adecuada para la gestión de vulnerabilidades en entornos académicos.

2.1 METODOLOGÍA

Nessus opera bajo un modelo cliente-servidor, donde el servidor (nessusd) es responsable de realizar las pruebas de vulnerabilidad y los clientes son utilizados en los puntos finales para configurar y lanzar escaneos específicos (Kak, A., 2024).

El servidor necesita estar en la misma subred que las máquinas virtuales que se van a escanear. Nessus realizará escaneo de puertos para identificar los servicios y verificar vulnerabilidades conocidas a través de una base de datos de *plugins,* una colección central de *scripts* y algoritmos que el escáner utiliza para detectar vulnerabilidades específicas en sistemas y redes. La eficacia de Nessus reside en esta base de datos de *plugins*, por lo que es de suma importancia realizar actualizaciones de manera periódica para poder detectar vulnerabilidades recién descubiertas.

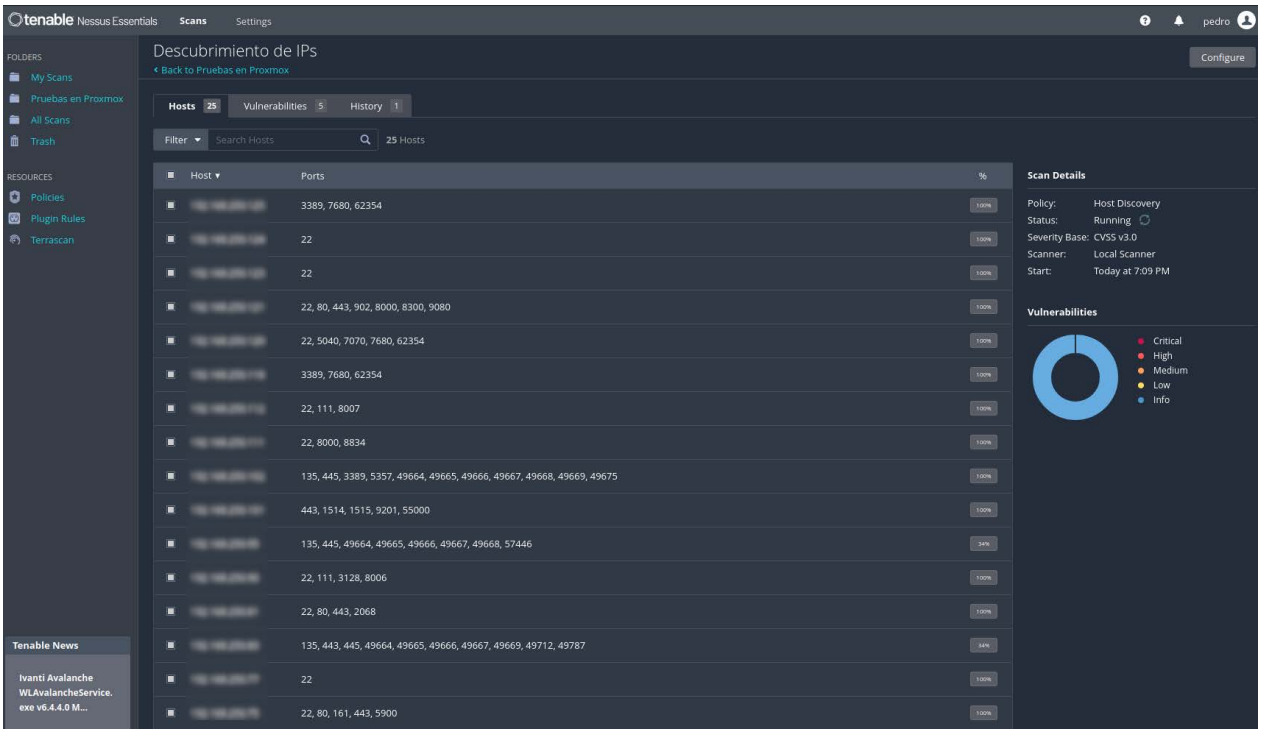
Implementación de Nessus en el hipervisor Proxmox

Dentro de un clúster de pruebas, se instaló el hipervisor Proxmox y, en él, se instalaron máquinas virtuales corriendo diversos sistemas operativos. Se utilizaron versiones desactualizadas de Ubuntu Server para poder encontrar algunas alertas de seguridad. También se instalaron máquinas virtuales con Windows Server. Dentro de una máquina virtual en el hipervisor, se instaló la herramienta de análisis de vulnerabilidades Nessus versión 6.3, en la misma subred que las máquinas virtuales a analizar. En la Figura 1, es posible ver cómo, en un primer escaneo, la herramienta nos muestra información inicial de las máquinas visibles en el segmento de red, así como los puertos abiertos.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 85 - 90

Figura 1

Escaneo general del segmento de red



Se optó por esta configuración para que sea más fácil evaluar todas las capacidades de la herramienta. Se instaló la versión más reciente de Nessus Essentials, que es una versión gratuita, de uso no comercial y que permite escanear direcciones IP en el momento de las pruebas. Durante la instalación, se configuraron direcciones IP estáticas para asegurar una comunicación consistente con las máquinas objetivo. No se realizaron configuraciones especiales adicionales en la instalación de Nessus más allá de la configuración inicial del administrador y la activación de la licencia.

Configuración y ejecución de los escaneos de vulnerabilidades

Nessus cuenta con una gran variedad de tipos de escaneo, como se muestra en la Tabla 1. Se eligieron aquellos adaptados a los sistemas operativos de las máquinas objetivo. Se llevaron a cabo escaneos de red básicos (*Basic Network Scan*) complementados con escaneos con credenciales (*Credentialed Scan*), proporcionando las credenciales de administrador correspondientes. El uso de éstos últimos permite a Nessus obtener una visión más profunda de la configuración del sistema operativo y las aplicaciones instaladas, lo que mejora la precisión de la detección de vulnerabilidades.

Se utilizaron los rangos de puertos predeterminados para los escaneos básicos. No se deshabilitaron *plugins* específicos, lo que permitió que Nessus utilizara su conjunto completo de pruebas de vulnerabilidad.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 86 - 90

Tabla 1

Tipos de escaneos de Nessus

Incluidos en Nessus Essentials	No incluidos en Nessus Essentials
Host Discovery	Web Application Tests
Basic Network Scan	Audit Cloud Infrastructure
Advanced Scan	Internal PCI Network Scan
Advanced Dynamic Scan	MDM Config Audit
Malware Scan	Offline Config Audit
Mobile Device Scan	PCI Quarterly External Scan
Credentialed Patch Audit	Policy Compliance Auditing
Active Directory Starter Scan	SCAP and OVAL Auditing
Find AI	

Consideraciones de seguridad al ejecutar Nessus en el mismo hipervisor

Al ejecutar Nessus dentro del mismo hipervisor Proxmox donde residen los servidores analizados, se deben tener ciertas consideraciones de seguridad. Una de las principales preocupaciones es la utilización de recursos. La ejecución de escaneos de vulnerabilidades puede consumir una cantidad significativa de recursos de CPU, memoria y red, lo que podría afectar el rendimiento de otras máquinas virtuales que se ejecutan en el mismo hipervisor (Proxmox Support Forum, 2023). Además, existe un riesgo de que una instancia de Nessus comprometida pueda ser utilizada para atacar otras máquinas virtuales o el propio hipervisor. Sin embargo, esta configuración también podría ofrecer algunas ventajas, como una mejor visibilidad de la red dentro del entorno virtual, lo que podría mejorar la precisión de los escaneos. Para mitigar los riesgos, es crucial asegurar la instancia de Nessus que se ejecuta en el entorno de producción y aplicar las mismas prácticas de seguridad que se utilizarían con cualquier otro servidor, como mantener el sistema operativo y las aplicaciones actualizadas, implementar controles de acceso y utilizar contraseñas seguras (GeeksforGeeks, 2024).

Identificación y clasificación de vulnerabilidades

Nessus utiliza el sistema de puntuación CVSS (*Common Vulnerability Scoring System*), uno de los estándares más reconocidos de la industria, diseñado para evaluar y comunicar la gravedad de las vulnerabilidades de seguridad en los sistemas informáticos, para clasificar la gravedad de cada vulnerabilidad detectada durante el escaneo (West Virginia University, 2022). Esta clasificación ayuda a los usuarios a entender el potencial impacto de cada vulnerabilidad y a priorizar las acciones de remediación. Los niveles de gravedad propuestos por el fabricante (Tenable, 2025) que se encuentran en los resultados de Nessus se presentan en la Tabla 2.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 87 - 90

Tabla 2

Clasificación de gravedad de vulnerabilidades de Nessus

Crítica	CVSS 9.0-10.0	Estas vulnerabilidades representan el mayor riesgo, ya que pueden ser explotadas fácilmente por un atacante remoto no autenticado y podrían resultar en que el sistema afectado sea comprometido.
Alta	CVSS 7.0-8.9	Las vulnerabilidades de gravedad alta pueden permitir a usuarios locales obtener privilegios elevados, a usuarios remotos no autenticados, visualizar recursos que deberían estar protegidos y a usuarios remotos autenticados, ejecutar código arbitrario o causar una denegación de servicio.
Media	CVSS 4.0-6.9	Estas vulnerabilidades son más difíciles de explotar que las críticas o altas, pero aún podrían llevar a la vulneración del sistema bajo ciertas circunstancias específicas.
Baja	CVSS 0.1-3.9	Las vulnerabilidades de gravedad baja generalmente requieren condiciones muy específicas para ser explotadas o, si se explotan con éxito, tienen un impacto mínimo en el sistema
Informativa	CVSS 0	Este nivel no indica una vulnerabilidad real, sino que proporciona información general sobre la configuración del sistema y su funcionamiento.

Comprender estos niveles de gravedad es fundamental para poder priorizar eficazmente la remediación de las vulnerabilidades encontradas en las máquinas virtuales del clúster de pruebas. La estandarización de la clasificación de vulnerabilidades mediante el sistema CVSS facilita la comunicación y la priorización de los riesgos de seguridad entre diferentes equipos y partes interesadas, así como promueve el empleo de un lenguaje común y una métrica reconocida en la industria.

3. RESULTADOS

Para medir el éxito y la efectividad del análisis de vulnerabilidades realizado en la infraestructura de prueba del Centro de Datos, se deben considerar métricas clave. Estas métricas proporcionan una medida cuantitativa de los hallazgos y ayudan a rastrear el progreso hacia la mejora de la postura de seguridad. Algunos autores han estudiado métodos para correlacionar las métricas CVSS con los resultados de herramientas de código abierto (Sllame et al., 2021).

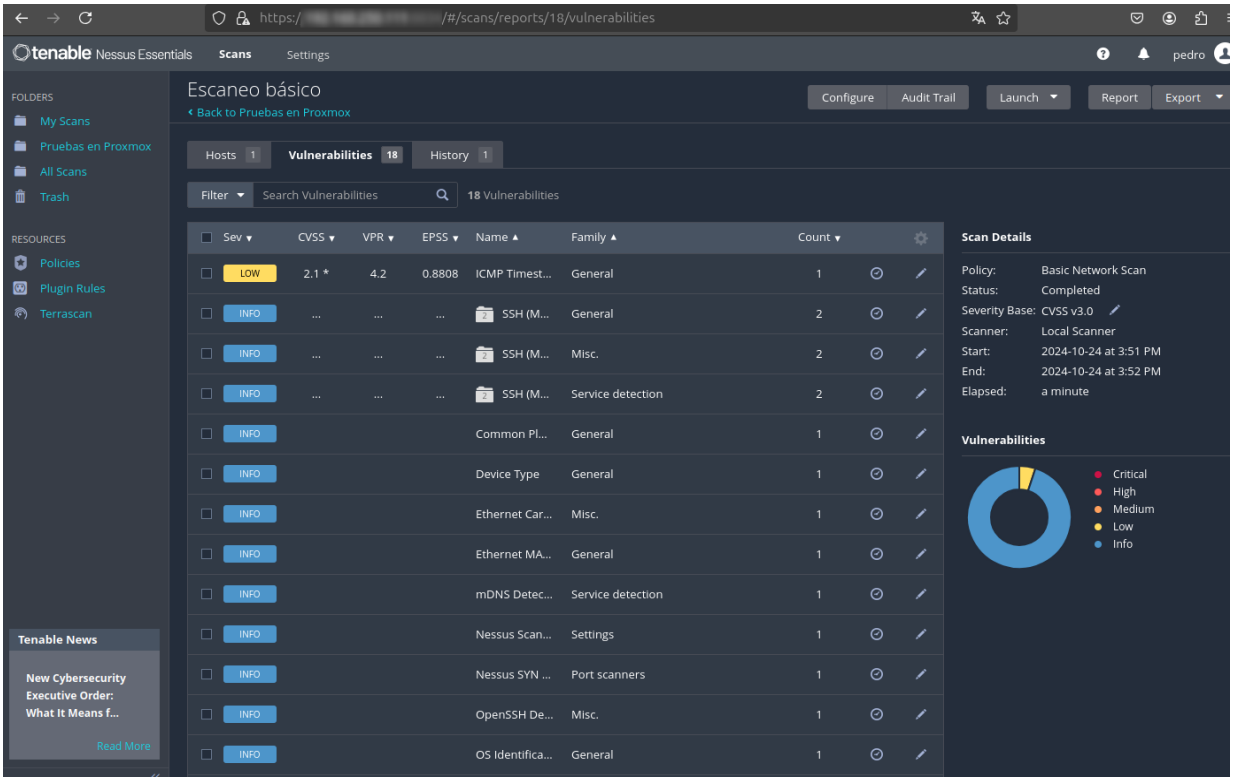
El número total de vulnerabilidades identificadas en todos los componentes escaneados de la infraestructura virtual fue una métrica principal. Esto proporcionó una indicación general del número de posibles debilidades de seguridad presentes. Además, la distribución de estas vulnerabilidades por nivel de gravedad (Crítica, Alta, Media, Baja, Informativa) ofreció información crítica sobre los riesgos más urgentes por atender. Un mayor porcentaje de vulnerabilidades críticas y de alta gravedad indicaría

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 88 - 90

una mayor necesidad de atención inmediata y esfuerzos de remediación. El número de vulnerabilidades únicas identificadas también se rastreó para comprender la diversidad de fallos de seguridad presentes, independientemente de cuántas veces apareciera una vulnerabilidad específica en diferentes activos. En la Figura 2, se muestra toda la información que nos presenta el panel de resultados de la herramienta. Es posible ver que la herramienta utiliza una interfaz intuitiva y ordenada que ayuda a identificar fácilmente el nivel de gravedad de cada alerta.

Figura 2

Panel de resultados de un escaneo básico



Si bien cada vulnerabilidad puede estudiarse de manera individual, existen casos de estudio que contemplan tablas de recomendaciones asociadas a distintas vulnerabilidades comunes (Paspuel y Pablo, 2024). Con base en esta información, junto con los resultados del análisis de Nessus, se realizaron las siguientes recomendaciones específicas para el entorno de pruebas:

- **Deshabilitar versiones obsoletas de TLS:** Deshabilitar inmediatamente TLS 1.0 y 1.1 en servidores web y sistemas operativos, así como forzar el uso de TLS 1.2 o superior, siguiendo las instrucciones específicas para cada servidor.
- **Reforzar la configuración SSH:** Revisar la configuración de SSH de los servidores. Revisar y aplicar políticas de contraseñas seguras para todos los usuarios de SSH. Considerar deshabilitar la autenticación basada en contraseñas, utilizar claves SSH en su lugar y evitar usar el puerto 22 predeterminado.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 89 - 90

- **Asegurar la configuración SNMP:** Cambiar la cadena de comunidad SNMP predeterminada en el segmento de red virtual a un valor privado seguro y restringir el acceso a estaciones de gestión autorizadas. Evaluar la viabilidad de actualizar a SNMPv3 para mejorar la seguridad.
- **Implementar encabezados de seguridad HTTP:** Configurar el servidor web que aloja la interfaz de gestión para incluir los encabezados Strict-Transport-Security (HSTS) y X-Frame-Options en sus respuestas HTTP, siguiendo la documentación de cada servidor web para obtener detalles de configuración.
- **Establecer un programa continuo de gestión de vulnerabilidades:** Implementar un cronograma para escaneos de Nessus regulares y automatizados de la infraestructura virtual. Establecer un proceso para revisar y remediar las vulnerabilidades identificadas en función de su gravedad.

Al implementar estas mejores prácticas y abordar las recomendaciones específicas derivadas del análisis de Nessus, se puede mejorar significativamente la postura de seguridad de las máquinas virtuales alojadas en el Centro de Datos.

4. CONCLUSIONES

El análisis realizado ha demostrado que Nessus puede ser un mecanismo de utilidad para la identificación y clasificación de vulnerabilidades en una infraestructura virtualizada compleja.

Nessus tiene la capacidad de descubrir un gran número de vulnerabilidades de seguridad de forma automática, una versión Professional o Expert la harían una solución viable para el escaneo en entornos con una gran cantidad de servidores virtuales y diversidad de sistemas operativos Windows, Linux y versiones recientes de macOS.

La clasificación de las vulnerabilidades por nivel de gravedad proporciona una visión clara de cuáles son los riesgos más graves que requieren atención inmediata. La presencia de vulnerabilidades en el entorno de pruebas, aunque esperado dada la inclusión de sistemas operativos desactualizados, recuerda la potencial exposición a amenazas significativas en un entorno de producción si alguno de los elementos de la infraestructura del Centro de Datos no se actualiza o configura debidamente, o si no se toman las medidas necesarias de detección.

Finalmente, se debe tener en cuenta que las recomendaciones, derivadas del análisis hecho por una herramienta de detección automatizada, serán sólo una parte de las medidas de seguridad necesarias. La adopción de mejores prácticas y cumplimiento de las políticas de seguridad establecerán un entorno propicio para la detección y respuesta ante futuras amenazas, lo que fortalece la resiliencia de la infraestructura digital que soporta el desarrollo de actividades sustantivas de la Universidad.

REFERENCIAS

Chhillar, K. (2021). *University computer network vulnerability assessment using NESSUS*. Paper Code: RDMOCS-P62. https://www.researchgate.net/publication/356998084_University_Computer_Network_Vulnerability_Assessment_using_NESSUS_Paper_Code_RDMOCS-P62

Elastic. (s.f.). ¿Qué es la gestión de vulnerabilidades? https://www.elastic.co/es/what-is/vulnerability-management

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.121 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 90 - 90

GeeksforGeeks. (2024). *Explain Nessus Tool in Security Testing.* https://www.geeksforgeeks.org/explain-nessus-tool-in-security-testing/

Harvard University Information Technology Security Operations. (2024). *HUIT Server security requirements standard v1.5*. https://enterprisearchitecture.harvard.edu/sites/hwpi.harvard.edu/files/enterprise/files/huit_server_security_requirements_standard_v1.5.pdf

Kak, A. (2024). *Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing*. Purdue University. https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture23.pdf

Lim, J. T., & Nieh, J. (2020). *Optimizing nested virtualization performance using direct virtual hardware*. In Proceedings of the Twenty-Fifth International Conference on *ASPLOS Architectural Support for Programming Languages and Operating Systems* (pp. 557-574). https://www.cs.columbia.edu/~nieh/pubs/asplos2020_dvh.pdf

Paspuel, T., & Pablo, J. (2024). *Propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades.* Universidad Tecnológica Israel. Paper Code: MASTER-SEG.INF-PRO;012. (pp. 56-63).

Proxmox Support Forum. (2023). *Compatibility with vulnerability scanners [Mensaje en un foro].* https://forum.proxmox.com/threads/compatibility-with-vulnerability-scanners.120807/

Railkar, D. (2022). A Study on Vulnerability Scanning Tools for Network Security. *International Journal of Scientific Research in Computer Science Engineering and Information Technology.* 8(6):340. (pp. 68-75). https://www.researchgate.net/publication/361951998_A_Study_on_Vulnerability_Scanning_Tools_for_Network_Security

Sllame, A. M., Tomia, T. E., & Rahuma, R. M. (2024). A Holistic Approach for Cyber Security Vulnerability Assessment Based on Open Source Tools: Nikto, Acunitx, ZAP, Nessus and Enhanced with AI-Powered Tool ImmuniWeb. In 2024 IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA) (pp. 68-75).

University of California, Berkeley. (2025). Frequently asked questions. Information security office. https://security.berkeley.edu/faq-page_

University of Texas at Austin. (2021). *Minimum security standards for systems.* https://security.utexas.edu/content/min-security-standards/systems

Tenable, Inc. (2025). *Risk metrics*. https://docs.tenable.com/nessus/Content/RiskMetrics.htm

West Virginia University. (2022). *Vulnerability management standard.* https://it.wvu.edu/policies-and-procedures/security/vulnerability-management-standard

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 91 - 107

Diseño e implementación de una solución híbrida para pruebas de desempeño a formularios dinámicos de software libre: metodología, arquitectura y herramientas

Información del reporte:

Para citar este reporte técnico:

Rangel Cano et al. (2025). Diseño e implementación de una solución híbrida para pruebas de desempeño a formularios dinámicos de software libre: metodología, arquitectura y herramientas. *Cuadernos Técnicos Universitarios de la DGTIC, 3* (3) páginas(91 - 107).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123

Liliana Rangel Cano
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
lilianarc@unam.mx
ORCID: 0009-0001-4100-4011

Cristhian Eder Alavez Barrita
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
calavez@comunidad.unam.mx
ORCID: 0009-0003-7408-2432

Resumen

El presente reporte técnico describe una experiencia en la aplicación de pruebas de desempeño a un formulario generado en la herramienta LimeSurvey por una entidad de la Universidad Nacional Autónoma de México. Las pruebas fueron aplicadas mediante una metodología conformada por las fases: planeación, diseño, aplicación y cierre, alineadas a actividades basadas en buenas prácticas. Durante el desarrollo de las actividades, se encontraron desafíos significativos en la automatización de pruebas, como son: el manejo de archivos adjuntos, de *tokens* de seguridad y la lógica condicional en los formularios. Para superar algunos de estos obstáculos, se desarrolló una solución que integró múltiples tecnologías: JMeter, WebDriver Sampler y Selenium WebDriver. Pese a ciertas limitaciones técnicas, la falta de información detallada de los componentes y del funcionamiento interno del

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 92 - 107

software, la solución fue viable para cumplir el objetivo de evaluar el desempeño de la aplicación al ajustar la estrategia con los recursos disponibles. Este reporte destaca la importancia de mantener un enfoque flexible al aplicar pruebas de desempeño de aplicaciones web complejas, lo cual sugiere que las estrategias híbridas pueden ser efectivas en ciertos contextos.

Palabras clave:

Pruebas de desempeño, scripts de automatización, LimeSurvey, Selenium WebDriver Sampler, JMeter.

Abstract

This technical report describes an experience applying performance testing on a form generated with the LimeSurvey tool by an entity at the National Autonomous University of Mexico. The tests were applied using a methodology comprised of the following phases: planning, design, implementation, and closure, aligned with activities based on best practices. During the development of the activities, significant challenges were encountered in test automation, such as the handling of attachments, security tokens, and conditional logic in forms. To overcome some of these obstacles, a solution was developed that integrated multiple technologies: JMeter, WebDriver Sampler, and Selenium WebDriver. Despite certain technical limitations and the lack of detailed information about the components and the internal workings of the software, the solution proved viable to achieve the objective of evaluating the application's performance by adjusting the strategy to the available resources. This report highlights the importance of maintaining a flexible approach when applying performance testing to complex web applications, suggesting that hybrid strategies can be effective in certain contexts.

Keywords:

Performance testing, automation scripts, LimeSurvey, Selenium WebDriver Sampler, JMeter.

1. INTRODUCCIÓN

En el panorama digital actual, es imprescindible considerar las características de calidad (atributos que determinan si una aplicación es rápida, confiable y usable) al evaluar un software, ya que éstas son fundamentales para el éxito de los proyectos. Entre ellas, se encuentra la eficiencia de desempeño, que mide qué tan rápido responde el software y cuántos recursos del sistema consume para realizar sus funciones. Esta característica es importante porque los usuarios esperan interacciones fluidas y tiempos de carga rápidos; cualquier retraso puede disminuir la satisfacción del cliente. Un retraso de tan solo un segundo en la respuesta de una página puede reducir esta satisfacción en un 16% (Mărcuță, 2024).

Las pruebas de desempeño son fundamentales para garantizar la calidad y eficiencia del software, ya que permiten evaluar su comportamiento bajo condiciones de estrés y uso intensivo de recursos, además de que aseguran un desempeño óptimo dentro de parámetros específicos de tiempo y rendimiento (International Organization for Standardization & International Electrotechnical Commission, 2011). De acuerdo con Legramante *et al.* (2020), su importancia radica en la capacidad para simular escenarios de carga y estrés, lo que permite prever posibles fallos y mejorar la experiencia del usuario, evitando problemas como tiempos de respuesta lentos. Por su parte, ImpactQA (s. f.) señala que aplicarlas ayuda a prevenir la disminución de ingresos, frustración en los usuarios y a mitigar riesgos reputacionales.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 93 - 107

Además, organismos internacionales como Micro Focus, Sogeti y Capgemini (World Quality Report 2023-24, 2023) destacan que las pruebas de desempeño son esenciales para garantizar la calidad técnica y la satisfacción del usuario.

LimeSurvey es una herramienta de encuestas en línea que, de acuerdo a lo indicado en su página, cuenta con más de 1.5 millones de usuarios a nivel mundial (Limesurvey, s. f.) para recolectar datos mediante una plataforma que permite a los usuarios diseñar encuestas personalizadas; su naturaleza de código abierto favorece la personalización, el desarrollo colaborativo y el soporte comunitario. En la Universidad Nacional Autónoma de México (UNAM), LimeSurvey es utilizada en actividades académicas y administrativas, evaluaciones estudiantiles, investigaciones y recolección de datos en proyectos sociales (Holguín, 2020).

En este marco, una entidad de la UNAM determinó utilizar LimeSurvey Community Edition versión 6.5.9 para atender el registro de propuestas de proyectos mediante un formulario, y así proyectar un escenario de 100 usuarios concurrentes al cierre del registro.

Para garantizar la respuesta a los usuarios que realizaron el registro de sus propuestas de proyecto de manera concurrente, generalmente en la última hora de la fecha límite del registro, y recopilar adecuadamente la información asociada de los proyectos, la entidad universitaria, basada en el conocimiento de la importancia de las pruebas de desempeño, identificó la necesidad de realizar pruebas de este tipo, que tenían como objetivo evaluar la estabilidad de la plataforma ante un escenario de 100 usuarios en carga sostenida y conocer los límites de atención con los recursos de infraestructura disponibles. Por lo anterior, solicitó el apoyo técnico para su realización y proporcionó los insumos necesarios para las pruebas (ambiente tecnológico de pruebas), entre los que se encontraba el apoyo de especialistas con disponibilidad para aclarar dudas estructurales del software, así como para atender cualquier eventualidad.

Dado que la plataforma fue desarrollada externamente a las área universitarias involucradas en la aplicación de las pruebas de desempeño, la automatización de las actividades a simular presentó un desafío técnico significativo, debido a la falta de información detallada de los componentes y del funcionamiento interno del software, lo que dificultó la identificación de los procesos clave y la realización de ajustes.

El presente reporte técnico tiene como objetivo describir tanto la metodología utilizada como las actividades realizadas para la aplicación de las pruebas de desempeño al cuestionario, así como indicar la manera en que se resolvió el problema técnico en la automatización de las pruebas.

2. DESARROLLO TÉCNICO

Las pruebas de desempeño permiten realizar una evaluación al software tanto para medir su rendimiento bajo diversas condiciones de concurrencia, carga, volumen y/o estrés, como para identificar el comportamiento del software en términos de velocidad, estabilidad y capacidad de respuesta, ya que son un tipo de prueba para determinar la eficiencia de rendimiento de un componente o sistema (Bath et al., 2018). Se comprendió la aplicación de la siguiente metodología establecida (Molyneaux, 2014), la cual puede definirse como un conjunto estructurado de actividades y técnicas que se utilizan para evaluar la eficacia en la simulación de 100 usuarios concurrentes al resolver un formulario compuesto de diversos elementos de captura.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 94 - 107

Consideraciones éticas

Antes de hablar de la metodología empleada, se destaca que las pruebas de desempeño deben realizarse únicamente a solicitud y con autorización expresa de los responsables del proyecto, con objetivos claros y definidos para el beneficio del mismo, debido a los riesgos asociados con su aplicación, tales como: la consulta o generación de información sensible, la posible degradación del rendimiento o la caída tanto del servicio evaluado como de otros servicios que coexisten en la misma infraestructura o con los que se comunica. En caso de que el software evaluado se comunique con otros sistemas o servicios, también debe existir la aprobación de los responsables de dichos servicios.

Las pruebas deben llevarse a cabo en un ambiente tecnológico específico para tal fin; si se realizan en el ambiente productivo, es indispensable contar con respaldos completos y un plan de mitigación de riesgos para evitar impactos negativos.

Los especialistas encargados de las pruebas deben informar sobre el proceso, los riesgos y las implicaciones de estas actividades, planificándolas cuidadosamente para incluir respaldos de información, seleccionar momentos oportunos que minimicen el impacto tanto en el servicio evaluado como en los que comparten infraestructura, y establecer mecanismos de seguridad compensatorios. Además, se debe evitar comprometer la integridad y confidencialidad de la información, haciendo uso exclusivo de datos de prueba cuando sea posible.

Metodología

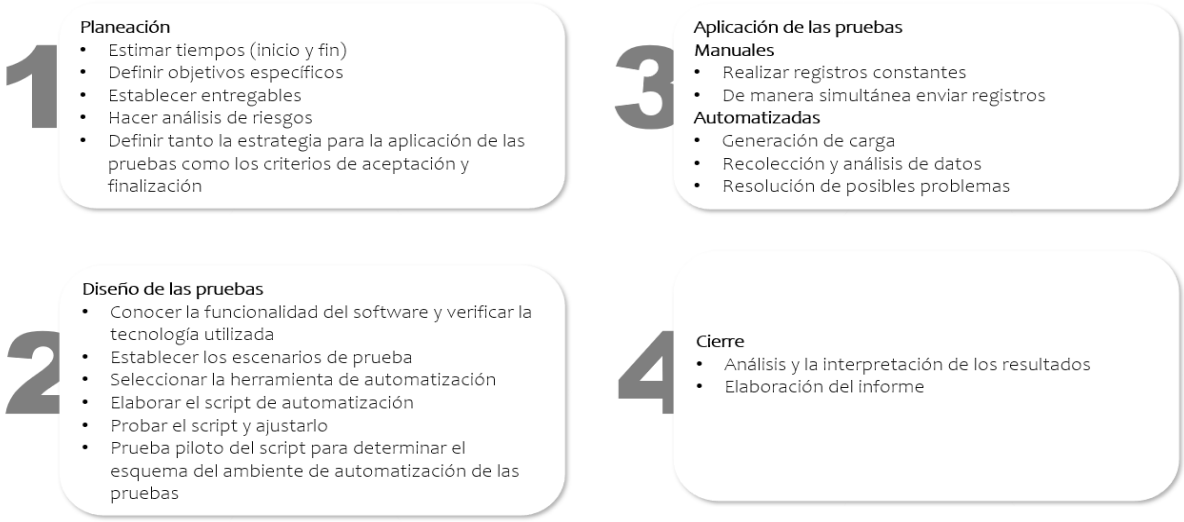
A continuación, como se muestra en la Figura 1, se presentan las fases y buenas prácticas que se llevaron a cabo en la aplicación de pruebas de desempeño del formulario generado en la herramienta LimeSurvey, con énfasis en las actividades que presentaron mayores desafíos. Aunque las fases no se denominan exactamente como en el *Foundation Level Specialist Syllabus Performance Testing* del ISTQB (Bath et al., 2018), las tareas se alinean con las definidas en el *syllabus*: "Planeación", "Análisis, diseño e implementación", "ejecución" y "análisis y reporte de resultados".[1]

1 Las actividades del *Syllabus* denominadas "Planeación", "Análisis, diseño e implementación", "Ejecución" y "Análisis y reporte de resultados" corresponden respectivamente a las fases de "Planeación", "Diseño de pruebas", "Aplicación de las pruebas" y "Cierre" en la metodología propuesta.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 Vol. 3, Núm. 3. julio-septiembre 2025, págs. 95 - 107

Figura 1

Metodología aplicada en las pruebas de desempeño



Entre el 10 y el 28 de junio de 2024, se llevó a cabo el proceso de pruebas de desempeño, en el cual, la etapa de diseño ocupó la mayor parte del tiempo disponible, representando un 80% del total (12 de los 15 días hábiles). Esta fase fue clave para identificar y desarrollar la solución tecnológica adecuada, centrada en la automatización de las pruebas. Durante este periodo, se llevaron a cabo actividades como la búsqueda de información relevante, la selección de herramientas apropiadas, así como la elaboración y configuración del *script* de automatización.

2.1 PLANEACIÓN

La planeación de las pruebas de desempeño fue tratada como un proyecto, específicamente, en actividades de estimación de tiempos (inicio y fin), definición de objetivos específicos, asignación de recursos y establecimiento de entregables.

En el caso concreto de las pruebas de desempeño al formulario, la actividad con mayor relevancia, debido al desarrollo y los resultados de éstas, fue la definición tanto de la estrategia para su aplicación como de los criterios de aceptación y finalización de las mismas.

Conforme a las buenas prácticas del sector y a las recomendaciones del Programa de estudios *Certified Performance Tester* con *JMeter* (Echeverria et al., 2019), se establecieron los criterios de aceptación para las pruebas de desempeño. Según este programa, es importante definir uno o más criterios u objetivos a alcanzar, los cuales pueden basarse en la cantidad de operaciones a ejecutar en un intervalo de tiempo, al consumo de recursos del sistema o al tiempo de respuesta de cada transacción, medidos bajo condiciones de carga definidas por el escenario correspondiente. Una vez que se cumplen los criterios de aceptación, las pruebas se dan por finalizadas.

Un desacierto que se cometió al definir la estrategia fue considerar como viable la automatización del flujo funcional de las pruebas, debido a que este proceso fue factible en proyectos previos con diversas

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 96 - 107

tecnologías. Por lo anterior, la estrategia tuvo que ser ajustada, conforme se desarrollaron las actividades, al plantear un esquema que incluyó la aplicación de pruebas manuales para adjuntar archivos y pruebas automatizadas para el ingreso de la información.

Un acierto que debe mantenerse en futuros proyectos es puntualizar la definición de los criterios de aceptación y finalización de las pruebas, que incluyan los escenarios favorables y desfavorables, para evitar prolongar las actividades sin obtener beneficios adicionales y/o cambios en los resultados de las pruebas.

Como lecciones aprendidas que se podrán considerar en proyectos que involucren pruebas de desempeño, se identificaron principalmente las siguientes:

- Considerar en el análisis de riesgos la inviabilidad de automatizar todos los movimientos realizados por el usuario (aun cuando se hayan realizado en proyectos previos); la manera de implementar y estructurar el código fuente del software pueden ser un obstáculo importante en la automatización.
- En la asignación de recursos humanos, contemplar como factor clave de éxito del proyecto, involucrar y establecer como compromiso la disponibilidad y participación del equipo de desarrollo en la automatización.
- En la estimación de tiempo, tomar en consideración que, debido a que cada proyecto es diferente, la automatización está asociada a la complejidad, tecnología utilizada y la estructura del código fuente, por lo que la duración de esta actividad puede variar incluso semanas.

2.2 DISEÑO DE LAS PRUEBAS

En las siguientes secciones, se presentan las actividades de preparación para la aplicación de pruebas que se contemplaron durante el diseño de las mismas:

2.2.1 CONOCER LA FUNCIONALIDAD DEL SOFTWARE Y VERIFICAR LA TECNOLOGÍA UTILIZADA

El formulario bajo pruebas fue generado en la plataforma de software libre y de código abierto LimeSurvey, la cual permite crear y administrar formularios en línea. Dicha plataforma posibilita diseñar cuestionarios, guardar las respuestas de los usuarios y analizar los resultados, a la vez que permite la personalización de los cuestionarios creados con preguntas condicionadas y múltiples tipos de respuestas; además, brinda la posibilidad de exportar los datos obtenidos.

El formulario se organizó en 6 páginas, cada una incluyendo entre 1 y 10 preguntas, con la información distribuida en un mínimo de 38 preguntas. Cada una solicitaba el ingreso de información mediante elementos como listas desplegables, opciones de selección única, casillas de verificación, campos para capturar datos y la posibilidad de adjuntar archivos.

Para definir las pruebas y determinar la manera de abordarlas, fue necesario conocer las condiciones en las que se encontraba el software, asegurar tener una versión estable sin errores de funcionamiento en el flujo principal y/o en los movimientos a realizar por el usuario e identificar las validaciones en los datos solicitados para evitar fallos en la generación del *script* de automatización o en la ejecución de las pruebas a causa de ingresar datos inválidos.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 97 - 107

2.2.2 ESTABLECER LOS ESCENARIOS DE PRUEBA A AUTOMATIZAR

El objetivo de las pruebas era conocer el comportamiento del formulario al ser contestado de manera concurrente, por lo que el único escenario seleccionado fue simular el flujo para contestarlo.

Se descartó la aplicación de pruebas relacionadas con la funcionalidad de LimeSurvey para gestionar cuestionarios o usuarios, obtención de resultados y estadísticas, como cualquier otra función complementaria. Esto se debió a que el objetivo principal no era evaluar la herramienta en su totalidad, sino centrarse exclusivamente en el comportamiento del formulario.

2.2.3 SELECCIÓN DE LA HERRAMIENTA DE AUTOMATIZACIÓN

Se eligió esta herramienta para la automatización de las pruebas debido a la experiencia en el uso de la herramienta JMeter para capturar información y adjuntar archivos, además de que cuenta con una comunidad y material de apoyo extenso.

JMeter es una aplicación de código abierto diseñada para realizar pruebas de carga y medir el rendimiento de aplicaciones web (Apache JMeter, s. f.). Su versatilidad permite simular múltiples usuarios y generar cargas significativas en el sistema, lo que resulta ideal para evaluar cómo responde el software bajo condiciones específicas.

2.2.4 ELABORAR EL SCRIPT DE AUTOMATIZACIÓN

Una vez seleccionada la herramienta *JMeter*, se creó un primer *script* de automatización[2] basado en las prácticas de grabación y ejecución para *scripts* avanzados, como la parametrización, tiempos de espera, controladores lógicos, aserciones y depuración del *script*, propuestas en el programa de estudios PtU (Echeverria et al., 2019). Este *script* se generó mediante la grabación y reproducción de las interacciones de los usuarios con el formulario de manera tradicional. Durante este proceso, se identificó que los elementos dinámicos, como algunos que utilizan *JavaScript*, no se integran adecuadamente.

Dado que se identificó una complejidad difícil de acotar, se solicitó apoyo a la entidad universitaria en:

- Proporcionar formularios con preguntas con elementos de captura específicos, para abordar la automatización de las pruebas de desempeño y con el propósito de analizar de manera aislada la manera de automatizar cada pregunta; se utilizaron formularios simples y estructurados con preguntas básicas, lo que permitió centrarse en la funcionalidad de cada campo de manera individual, de modo que se acotaron los puntos y variables involucrados en la funcionalidad del sistema.
- Acompañamiento en la solución de los problemas presentados en los *scripts* de automatización mediante asesoría respecto a la forma en que se encontraba estructurado el código fuente en ciertas funciones, apoyo para realizar ajustes en el código y en el monitoreo de *logs* para poder solucionar los problemas asociados.
- El apoyo proporcionado por la entidad universitaria se enfocó en comprender la funcionalidad LimeSurvey para identificar posibles soluciones a los errores presentados en el *script* de automatización, actividad que involucró tiempo considerable.

2 *Script* de automatización es un código que contiene un conjunto de instrucciones para realizar una tarea, que reproducen la actividad de los usuarios al utilizar el sistema.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 Vol. 3, Núm. 3. julio-septiembre 2025, págs. 98 - 107

- En la Figura 2, se presenta un resumen de las incidencias identificadas durante el proceso de automatización de las pruebas, así como las soluciones implementadas para cada una. Estos aspectos se describen con mayor detalle en las secciones posteriores.

Figura 2

Desafíos y la solución generada en la elaboración del script de automatización

Desafío	Descripción	Solución
LimeSurveyutiliza JavaScript	Los elementos dinámicos, como algunos que utilizan JavaScript, no se integran adecuadamente	Integrar Selenium
Manejo de archivos adjuntos	LimeSurvey utiliza un modal para cargar archivos	Se ajustó la estrategia y se hicieron pruebas manuales
Gestión de sesiones y token de seguridad	LimeSurvey, implementa tokens CSRF que cambian constantemente durante las interacciones con el formulario	Parametrización del script
Formularios dinámicos	LimeSurvey permite incluir lógica condicional (preguntas que solo se muestran de acuerdo con las respuestas anteriores)	Establecer un flujo de información estático para todos los usuarios

En los formularios proporcionados por la entidad universitaria, que contenían elementos de captura específicos, se presentaron los siguientes problemas durante la generación de *scripts*:

Manejo de archivos adjuntos (Carga de archivos)

- LimeSurvey utiliza un modal para cargar archivos, lo que es un desafío al realizar pruebas de carga con herramientas como JMeter, ya que requiere interacción con la interfaz del formulario de manera dinámica para llevar a cabo la carga.

Gestión de sesiones y *tokens* de seguridad

- LimeSurvey implementa medidas de seguridad como los *tokens* CSRF para evitar ataques, estos *tokens* cambian constantemente durante las interacciones con el formulario, lo que dificulta la automatización de las pruebas de carga, ya que cada sesión o solicitud debe incluir un *token* válido. Si no se manejan correctamente, los *scripts* de prueba pueden fallar, ya que no pueden obtener ni mantener los *tokens* actualizados entre las interacciones.
- Si la plataforma no está configurada para mantener sesiones abiertas el tiempo suficiente para completar las pruebas, o si las sesiones expiran rápidamente debido a la inactividad, se pueden generar errores debido al "tiempo de sesión expirado".

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 99 - 107

Complejidad de formularios con condicionalidades y lógica

- LimeSurvey permite incluir lógica condicional (preguntas que sólo se muestran de acuerdo con las respuestas anteriores), lo que hace que los formularios sean dinámicos, esto aumenta la complejidad al simular múltiples usuarios.
- Las interacciones del usuario, como la selección de opciones de respuestas o la validación de campos, dependen de *scripts* JavaScript o elementos dinámicos; estas interacciones no siempre son susceptibles de automatización.

Compatibilidad con la herramienta de prueba de desempeño JMeter

- Al usar herramientas de pruebas como *JMeter*, simular múltiples usuarios simultáneos y su interacción con LimeSurvey es más complejo si el formulario depende de *JavaScript* o tiene interacciones dinámicas, debido a que no simulan la interfaz de usuario.
- LimeSurvey no está diseñado para pruebas de desempeño como prioridad, lo que significa que su integración con herramientas externas de prueba de carga o automatización (como *JMeter*) requiere trabajo exhaustivo.

Para dar solución a los problemas identificados, principalmente la complejidad en la simulación de interacciones con formularios dinámicos y la dificultad para manejar elementos como la carga de archivos, se llevó a cabo una revisión exhaustiva en diversos espacios de Internet con el objetivo de identificar soluciones y prácticas para llevar a cabo las pruebas de desempeño al formulario con *JMeter*. El proceso incluyó la consulta de recursos académicos, manuales oficiales de la herramientas LimeSurvey, artículos técnicos, así como de foros y discusiones en comunidades especializadas.

Como resultado de la revisión, se probaron diversas propuestas de solución planteadas para JMeter, sin obtener una solución que atendiera los problemas mencionados. Sin embargo, se identificaron trabajos como el de (Tufegdžić et al., 2021), en el que se aborda un marco híbrido para pruebas automatizadas a una aplicación de publicidad basada en web, con *Selenium* como componente central.

En este contexto, se decidió explorar soluciones alternativas para superar los desafíos presentados y *WebDriver* surgió como una solución viable, tras integrar el componente con *JMeter*, realizar pruebas y obtener resultados satisfactorios en la capacidad de interacción con los diferentes tipos de campos y formularios, superando la mayoría de las limitaciones previas. Esta estrategia híbrida permitió combinar la capacidad de *JMeter* para generar carga concurrente con la habilidad de *Selenium WebDriver* para controlar un navegador real, ejecutar *JavaScript* y manejar elementos dinámicos de la interfaz de usuario, para simular de forma más fiel la interacción del usuario final.

2.2.4.A IMPLEMENTACIÓN TÉCNICA

Para preparar el esquema del ambiente de automatización, se integraron diversas soluciones tecnológicas que abordaron las problemáticas presentadas en el funcionamiento de cada componente, como se muestra en la Figura 3.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 100 - 107

A continuación se detallan las soluciones implementadas:

Linux Mint

Como base del ambiente, se utilizó el sistema operativo Linux Mint 21.3, seleccionado debido a que su diseño y gestor de software permiten agilizar la instalación de paquetes, dependencias y aplicaciones.

OpenJDK

OpenJDK (*Open Java Development Kit*) es una implementación de código abierto de la plataforma Java que incluye el compilador, la máquina virtual (JVM) y las bibliotecas estándar. Proporciona un entorno libre y gratuito que cumple con los estándares de la plataforma Java y es ampliamente utilizado tanto en servidores como en aplicaciones de escritorio. Este componente permitió sustituir a JDK (software propietario de Oracle), que es requisito para el funcionamiento de *JMeter.*

WebDriver Sampler

El *WebDriver Sampler* (*Documentation :: JMeter-Plugins.org*, s. f.) permite automatizar la ejecución y recolección de métricas de desempeño en el navegador (lado del cliente), lo cual puede resolver algunos de los factores que complican la automatización mediante peticiones entre los que se encuentran:

- Ejecución de JavaScript en el lado del cliente, por ejemplo, AJAX y plantillas JS.
- Transformaciones CSS, por ejemplo, transformaciones de matriz 3D, animaciones.
- Plugins de terceros.

Este componente especializado actuó como un puente entre *JMeter* y *Selenium WebDriver*, lo que permitió integrar las capacidades de automatización de navegador de *Selenium* dentro del marco de pruebas de desempeño de *JMeter.*

Selenium WebDriver

Selenium (*The Selenium Browser Automation Project*, s. f.) es una suite de herramientas de código abierto diseñada para la automatización de pruebas en aplicaciones web. Permite simular la interacción de un usuario con una página web, al ejecutar pruebas en navegadores reales de forma automática. Soporta múltiples lenguajes de programación como Java, Python, C# y *JavaScript*, lo que lo convierte en una opción flexible para diferentes ambientes de desarrollo. Con *Selenium*, es posible automatizar acciones como hacer clic en botones, rellenar formularios, navegar entre páginas y verificar el comportamiento de la interfaz de usuario.

WebDriver es una interfaz que permite la introspección y el control de agentes de usuario. Proporciona un protocolo de comunicación independiente de la plataforma y el lenguaje para que los programas fuera de proceso instruyan remotamente el comportamiento de los navegadores web. Se ofrece un conjunto de interfaces para descubrir y manipular elementos del DOM en documentos web y controlar el comportamiento de un agente de usuario (*WebDriver*, s. f.).

Según Leotta *et al*. (2023), *Selenium WebDriver* se ha consolidado como la biblioteca de facto para desarrollar pruebas funcionales de extremo a extremo (E2E) de aplicaciones web.

Esta herramienta brindó la interfaz para controlar los navegadores mediante código al simular las interacciones reales de los usuarios en el navegador.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 101 - 107

Driver **(controlador)**

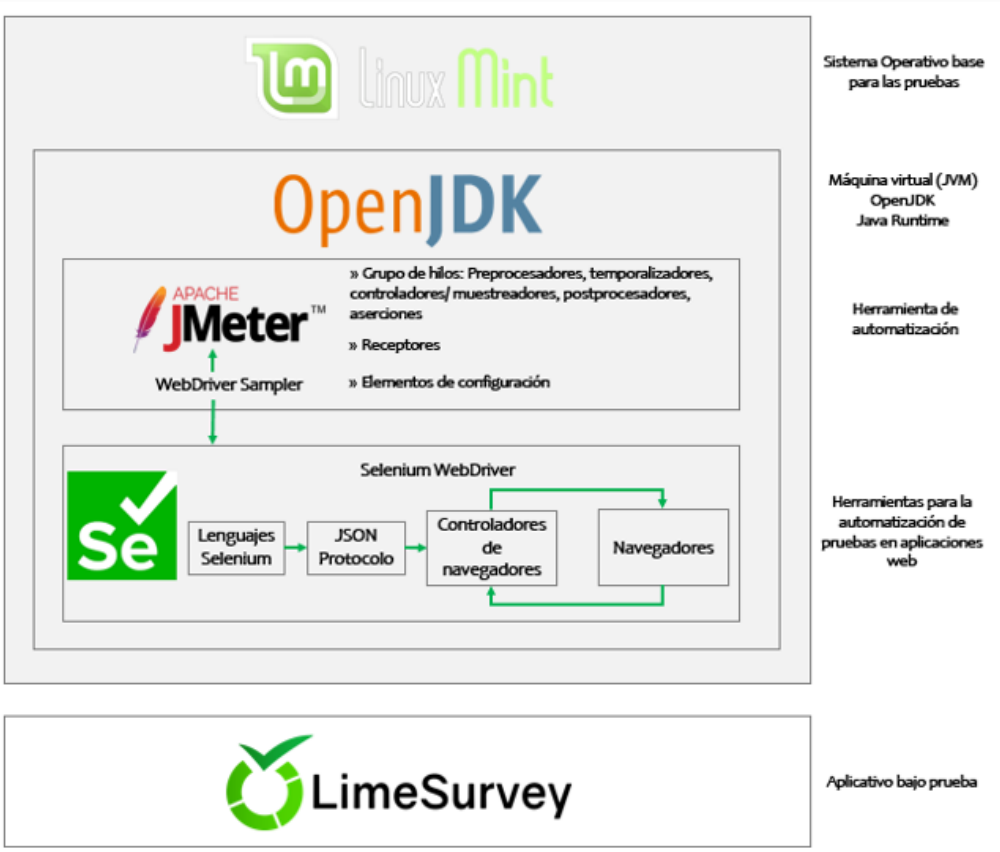
Para funcionar, *Selenium WebDriver* requiere un componente intermedio llamado *driver*, que controla el navegador y permite la interacción con la aplicación web. Cada proveedor de navegadores ofrece un *driver* específico para cada versión del navegador, lo que implica que los desarrolladores deben mantener alineadas las versiones del navegador y del *driver* para asegurar la compatibilidad (Leotta et al., 2023).

En este sentido, el *driver* desempeñó un papel esencial como intermediario entre *Selenium WebDriver* y el navegador. Este controlador implementó el protocolo W3C WebDriver y permitió que *Selenium WebDriver* se comunicara con Firefox, tradujo los comandos en acciones que el navegador pudo ejecutar, y proporcionó una capa de abstracción que facilitó la compatibilidad y estabilidad de la automatización.

Con la integración de estas tecnologías, se generó un ambiente de pruebas robusto y versátil; Linux Mint facilitó la instalación de OpenJDK, requisito de *JMeter*; el *WebDriver Sampler* proporcionó la infraestructura dentro de *JMeter*; *Selenium WebDriver* ofreció las capacidades de automatización del navegador; y el *driver* aseguró la comunicación con el navegador.

Figura 3

Arquitectura del ambiente para las pruebas de desempeño al formulario en LimeSurvey



https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 102 - 107

Una vez integrada la solución tecnológica para abordar la problemática presentadas en el *script* de automatización, se presentó un nuevo desafío significativo: aprender a codificar para *WebDriver*.

2.2.4.B CODIFICACIÓN

Otro de los retos en este proceso fue aprender a codificar en la interfaz, ya que requería la comprensión de su estructura y cómo interactuar con los navegadores. Para superar esta barrera, se dedicó tiempo a revisar diversas fuentes de información, como documentación oficial, tutoriales en línea, foros de desarrolladores y ejemplos prácticos. Si bien existen fuentes formales del tema, los métodos y recomendaciones no son exactos debido al cruce de tecnologías, por tal motivo fue necesario adoptar un enfoque de prueba y error[3], mismo que permitió experimentar directamente con el código para identificar la lógica de programación y los métodos para llevar a cabo las interacciones necesarias, así como adaptarlo al flujo de trabajo establecido.

Para la codificación, se determinó utilizar *Groovy*, el cual es un lenguaje de programación dinámico que se ejecuta sobre la máquina virtual de Java (JVM), que simplifica la escritura de *scripts* debido a su sintaxis concisa y fácilmente legible.

A partir del cambio de enfoque, la construcción de *scripts* cambió drásticamente, por lo que fue necesario escribir el código para cada interacción en el aplicativo. Esto implicó una nueva revisión del formulario para recolectar información de cada uno de los elementos involucrados en el flujo de trabajo: nombres, etiquetas, identificadores, argumentos y rutas, entre otros; así como los diversos eventos requeridos para replicar la funcionalidad: clics, desplazamientos, ingreso de datos, validaciones, entre otros movimientos.

Con los insumos identificados y registrados, la generación de *scripts* se llevó a cabo con la incorporación secuencial de los movimientos de cada sección del formulario, por lo que fue necesario validar y, en su caso, buscar varios elementos de interacción en tiempo de ejecución.

Es importante mencionar que esta solución resolvió únicamente los problemas asociados a elementos de captura solicitados como parte de la misma página, sin solventar la funcionalidad para adjuntar archivos.

Finalmente, se añadieron espacios de tiempo entre los movimientos a realizar, con la finalidad de que los elementos del formulario se encontraran presentes al interactuar con ellos.

2.2.5 PROBAR EL SCRIPT Y AJUSTARLO

A causa de los problemas presentados y a las soluciones generadas, en conjunto con la entidad universitaria, se acordó como estrategia para abordar las pruebas: cambiar el alcance de la automatización a la resolución del cuestionario y omitir los reactivos asociados a la importación de archivos.

3 La *prueba y error* es un proceso no lineal que implica experimentar repetidamente y explorar diferentes operaciones para aprender y utilizar aplicaciones de software complejas. Este método se basa en un ciclo de ejecución, evaluación y recuperación, permite a los usuarios identificar dificultades y explorar nuevas rutas para alcanzar sus objetivos, (Barbosa, 2022).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 103 - 107

2.2.6 PRUEBA PILOTO DEL SCRIPT PARA DETERMINAR EL ESQUEMA DEL AMBIENTE DE AUTOMATIZACIÓN DE LAS PRUEBAS

Una vez que el *script* de automatización funcionó adecuadamente con el nuevo alcance, se llevaron a cabo un conjunto de ejecuciones de éste para identificar la cantidad máxima de usuarios que se permitía simular desde el esquema del ambiente de automatización.

El máximo de usuarios que se pudieron simular por equipo fueron 20. Para lograr el objetivo esperado en las pruebas, se tuvo que replicar el esquema del ambiente de automatización en cinco equipos de cómputo.

Con la finalidad de poder distribuir las pruebas en diversos equipos, se generó una máquina virtual con la estructura del ambiente de pruebas, la cual integró las herramientas de automatización de pruebas de desempeño.

2.3 APLICACIÓN DE LAS PRUEBAS: MANUALES Y AUTOMATIZADAS

La aplicación de las pruebas estuvieron basadas y apoyadas en la planeación y en los productos de trabajo de control preparados en el diseño, para lo cual fue necesario que el formulario se encontrara en un ambiente análogo al productivo en cuanto a infraestructura y configuración se refiere.

Alineados a la nueva estrategia para realizar las pruebas de desempeño, en seguida se describen las actividades para la aplicación de las pruebas manuales y automatizadas.

2.3.1 APLICACIÓN DE LAS PRUEBAS MANUALES

Debido a la inviabilidad de automatizar las acciones para adjuntar archivos y a que el formulario presenta ventanas modales, tanto web como de sistema operativo, para esta tarea, se aplicó la prueba de manera manual, en conjunto con el personal de la entidad universitaria, la cual consistió en que, durante una hora, diversos usuarios realizaron registros de manera constante al formulario completo, incluida la importación de archivos de diferente extensión y tamaño. Para complementar la prueba y revisar la concurrencia, 10 usuarios ingresaron la información solicitada y, de manera relativamente simultánea, enviaron el registro.

Estas pruebas permitieron observar, desde la perspectiva del usuario final, el comportamiento del formulario e identificar el número de usuarios concurrentes que responde la plataforma. Adicionalmente, al personal de la entidad universitaria le permitió identificar acciones de respuesta en caso de materializarse el riesgo de que el formulario no responda adecuadamente a todos los usuarios por cuestiones de concurrencia.

2.3.2 APLICACIÓN DE LAS PRUEBAS AUTOMATIZADAS

Las pruebas automatizadas se realizaron a un formulario que omitió únicamente la funcionalidad para adjuntar archivos.

La aplicación de estas pruebas se llevó a cabo en un ciclo iterativo de *generación de carga*, *recolección y análisis de los datos* y *resolución de los posibles problemas*.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 104 - 107

En la *generación de carga,* se definió y aplicó la prueba con las características acordadas para cada prueba respecto al número de usuarios en concurrencia, tiempos de espera, entre otros elementos establecidos.

En la *recolección y análisis de los datos*, durante la ejecución de cada prueba, se monitoreó el comportamiento del sistema desde la interfaz visual de la herramienta de automatización, se observaron tanto las respuestas proporcionadas a los usuarios, como el registro en el *log* de la herramienta de automatización; al concluir la prueba, se verificó el registro de la información mediante la misma herramienta LimeSurvey. Adicionalmente, apoyados de personal de la entidad universitaria y en constante comunicación, se compartió la información del consumo de recursos de red, CPU y memoria RAM. Al término de cada prueba, se compartieron los resultados y, en conjunto, se determinó si la prueba fue exitosa o fallida[4].

En los casos donde los resultados de la prueba no fueron los esperados, en conjunto con el personal de la entidad solicitante y de un grupo de especialistas en redes y servidores, se verificó la causa-raíz del incidente y se determinaron e implementaron los pasos a seguir, tales como realizar ajustes pertinentes en la configuración en la infraestructura que soportaba el cuestionario.

Un factor de éxito fue llevar el control de las pruebas aplicadas, resultados obtenidos del monitoreo de recursos y el análisis de los mismos, lo que permitió comparar los resultados entre pruebas y determinar la mejor configuración para que la infraestructura responda adecuadamente al mayor número de usuarios en concurrencia.

2.4 CIERRE

Para concluir las pruebas, se llevó a cabo el análisis y la interpretación de los resultados obtenidos en cada una de las pruebas aplicadas y se documentaron en un informe que fue entregado a la entidad universitaria.

Como buenas prácticas, se realizó el *testware* del proyecto, el cual es el conjunto de productos de trabajo producidos durante el proceso de prueba para su uso en la planeación, diseño, ejecución, evaluación e informes sobre las pruebas. De acuerdo con Sosnówka (2013), el *testware* permite una gestión más eficiente de las pruebas, ya que proporciona una estructura organizada de todos los artefactos necesarios para planificar, diseñar y ejecutar pruebas, lo que facilita la identificación y resolución de problemas.

3. RESULTADOS

La aplicación de pruebas de desempeño al formulario desarrollado en la plataforma LimeSurvey presentó múltiples retos en la automatización, entre los cuales se destacan: la dificultad para abordar las pruebas debido al desconocimiento de la estructura del código fuente, ya que el desarrollo de la herramienta fue realizado por personal externo a los involucrados en las pruebas, y el tiempo necesario para encontrar una solución adecuada.

En la generación del *script* de automatización en *JMeter*, se presentaron problemas en el manejo de archivos adjuntos (carga de archivos), en la gestión de sesiones y uso *tokens* de seguridad, en las

4 Una *prueba exitosa* es en la que sus resultados corresponden a los esperados, mientras que una *prueba fallida* es aquella que no es concluida, presenta errores y/o no cumplen con los criterios de aceptación definidos.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 105 - 107

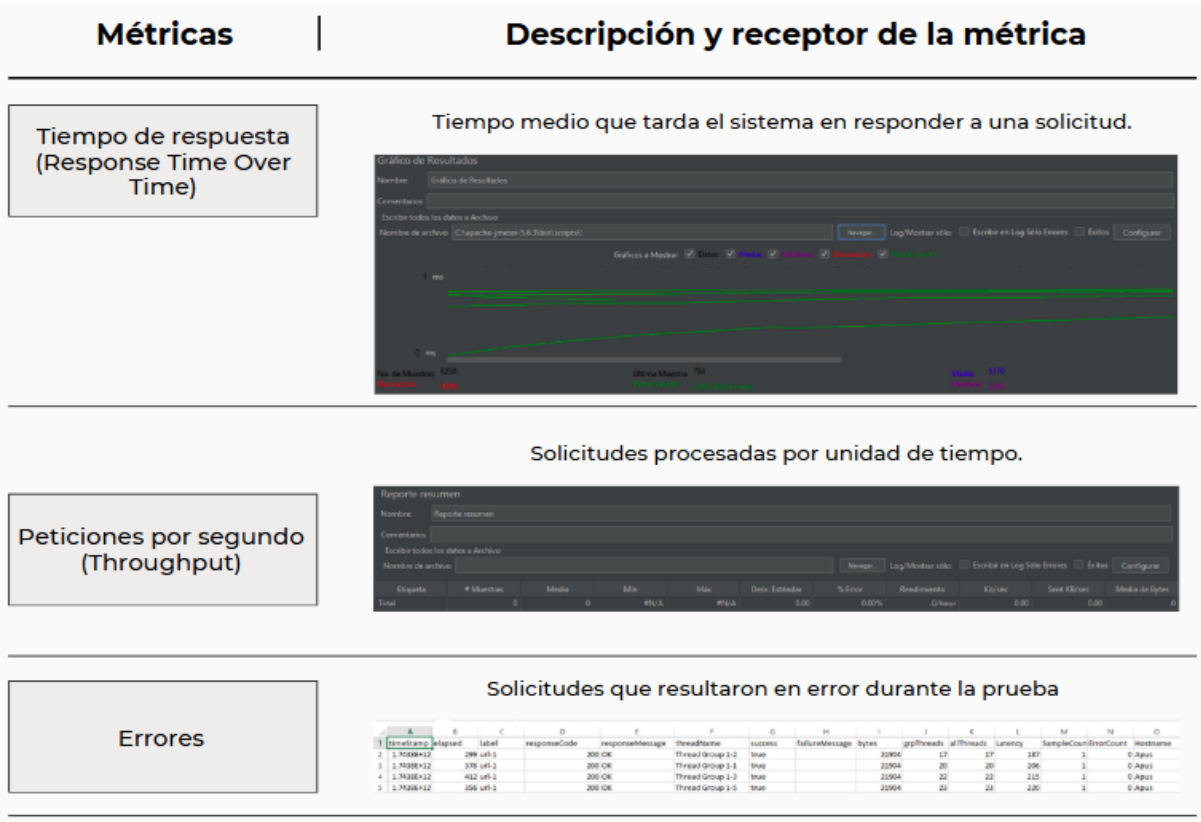
condiciones y lógica del formulario, así como en el funcionamiento interno de LimeSurvey que no era compatible con la herramienta de prueba de desempeño.

Aunque durante el proceso de preparación de las pruebas se presentaron algunos impedimentos que obstaculizaron la automatización, se abordaron la mayoría de problemas presentados al integrar diversas soluciones tecnológicas a *JMeter*, como *OpenJDK*, *WebDriver Sampler*, *Selenium WebDriver* y el *driver*. El único incidente que no fue resuelto fue la automatización en preguntas que requerían adjuntar archivos debido a que se solicitaban mediante ventanas modales dinámicas en *JavaScript*.

La Figura 4 presenta las principales métricas utilizadas para analizar los resultados obtenidos de las pruebas.

Figura 4

Algunas métricas de JMeter consultadas para el análisis de resultados de las pruebas



Ante la complejidad técnica de la solución implementada, se ajustó la estrategia para combinar pruebas de desempeño manuales y automatizadas, lo que permitió cumplir con el objetivo de conocer el comportamiento de la aplicación bajo condiciones específicas de concurrencia. Aunque la solución integrada requería un elevado consumo de recursos tecnológicos para simular la concurrencia, fue favorable que el número de usuarios a simular fuera relativamente pequeño y, por tanto, compatible con los recursos disponibles.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 106 - 107

Gracias a esta adaptación, se aplicaron las pruebas con los recursos tecnológicos y humanos disponibles, lo que garantizó resultados confiables y demostró que, incluso con restricciones técnicas, es posible alcanzar los objetivos planteados mediante una planificación flexible y eficiente.

La aplicación de pruebas de desempeño manuales permitieron observar el comportamiento del formulario al ser resuelto desde la perspectiva del usuario final, en carga de 27 usuarios al registrar información constante y adjuntar archivos de diversos tamaños y extensiones, mientras que las pruebas automatizadas mostraron el comportamiento del formulario en concurrencia de 100 usuarios.

4. CONCLUSIONES

Como elementos importantes a considerar que apoyarán a nuevos proyectos que involucren el desarrollo de pruebas de desempeño, destaca tener presente que automatizar toda la funcionalidad no siempre es la mejor solución para conocer el comportamiento del software. En este sentido, al considerar la automatización como única alternativa para las pruebas, es fundamental reconocer que cada funcionalidad puede requerir de un enfoque diferente y el uso de herramientas específicas.

La solución implementada para abordar las pruebas de desempeño al formulario en LimeSurvey, que integra *WebDriver* en *JMeter*, se enmarcó dentro de una metodología que permite una evaluación más precisa y detallada del comportamiento de la aplicación al simular las interacciones del usuario en un ambiente controlado de pruebas.

El esquema planteado permite replicar de manera fidedigna las acciones de los usuarios, como clics, desplazamientos y entradas de texto, lo cual es necesario al analizar aplicaciones que requieren una interacción dinámica. Además, es eficaz para aplicaciones que emplean tecnologías como *AJAX* o *JavaScript*, cuyas interacciones no pueden ser capturadas de manera adecuada en pruebas que sólo involucran solicitudes HTTP (como lo hace *JMeter* de manera independiente). Sin embargo, esta integración presenta limitaciones tecnológicas inherentes a su ejecución, la principal es que las pruebas basadas en *WebDriver* son considerablemente más costosas en términos de recursos y tiempo debido a la necesidad de interactuar con un navegador real, lo que aumenta la complejidad de la ejecución, especialmente cuando se requiere simular una gran cantidad de usuarios simultáneos.

El proyecto permitió adquirir nuevos conocimientos y destacó la importancia de considerar la integración de nuevas herramientas para la automatización de soluciones tecnológicas actuales. Esta experiencia no sólo amplió nuestra comprensión sobre las mejores prácticas en automatización, sino que también resaltó la necesidad de adaptar las herramientas a las características específicas de las aplicaciones.

REFERENCIAS

Apache JMeter—*Apache JMeter™*. (s. f.). Recuperado 23 de junio de 2025, de https://jmeter.apache.org/

Barbosa, S. (2022). *CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3491102

Bath, G., Black, R., Podelko, A., Pollner, A., & Rice, R. (2018). *Foundation Level Specialist Syllabus Performance Testing*.

Crear encuestas: LimeSurvey Herramienta de encuestas gratuita. (s. f.). Recuperado 23 de junio de 2025, de https://www.limesurvey.org/es

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.123 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 107 - 107

Documentation: JMeter-Plugins.org. (s. f.). Recuperado 23 de junio de 2025, de https://jmeter-plugins.org/wiki/WebDriverSampler/

Echeverria, D., Skrilec, G., Verma, R., Herrera, A., Fernández, A., Vivanco, A., Acevedo, Á. R., Brands, A., Acosta, B. M., Tolosa, D., Delgado, E. R., Sales, E. E., Henostroza, G., Sosa, G. M., Terrera, G., Revalcaba, H., Ortiz, J. P., Rios, J. P., Melendez, L., … Nane, S. (2019). *PtU Certified Performance Tester con JMeter (CPTJM)*.

Holguín Carrillo, R. (2020). Una caja de herramientas para medir el universo de protestas en México. *Revista Digital Universitaria*, *21*(3). https://doi.org/10.22201/codeic.16076079e.2020.v21n3.a2

International Organization for Standardization, & International Electrotechnical Commission. (2011). *ISO/IEC 25010:2011: Systems and Software Engineering—Systems and Software Quality Requirements and Evaluation (SQuaRE)—System and Software Quality Models*. ISO/IEC.

Legramante, G., Bernardino, M., Rodrigues, E. M., & Basso, F. (2020). Systematic Literature Review on Web Performance Testing. *Anais Da IV Escola Regional de Engenharia de Software (ERES 2020)*, 285-295. https://doi.org/10.5753/eres.2020.13739

Leotta, M., García, B., Ricca, F., & Whitehead, J. (2023). Challenges of End-to-End Testing with Selenium WebDriver and How to Face Them: A Survey. *2023 IEEE Conference on Software Testing, Verification and Validation (ICST)*, 339-350. https://doi.org/10.1109/ICST57152.2023.00039

Mărcuță, C. (2024, diciembre 5). *Understanding the Significance of Performance Testing and Why It is Essential for Your Software's Success*. https://moldstud.com/articles/p-understanding-the-significance-of-performance-testing-and-why-it-is-essential-for-your-softwares-success

Molyneaux, I. (2014). *The Art of Application Performance Testing: From Strategy to Tools*. O'Reilly Media.

Sosnówka, A. (2013). Testware Visualized—Visual Support for Testware Reorganization: *Proceedings of the 8th International Conference on Evaluation of Novel Approaches to Software Engineering*, 109-114. https://doi.org/10.5220/0004451001090114

The Selenium Browser Automation Project. (s. f.). Selenium. Recuperado 23 de junio de 2025, de https://www.selenium.dev/documentation/

Tufegdžić, M., Miodragović, G., & Aleksandrov, S. (2021). *Hybrid framework for automated testing of web application for advertisement*. Conference: Young science - Robotics and nano-technology of modern mechanical engineering, Donbass State Engineering Academy, Kramatprsk.

WebDriver. (s. f.). Recuperado 10 de abril de 2025, de https://www.w3.org/TR/webdriver1/

What is Performance Testing? The Complete Guide. (s. f.). *ImpactQA*. Recuperado 10 de abril de 2025, de https://www.impactqa.com/guides/performance-testing/

World Quality Report 2023-24. (2023, diciembre 8). *Capgemini*. https://www.capgemini.com/insights/research-library/world-quality-report-2023-24/

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 108 - 121

Comunicación IPv4 segura entre áreas universitarias a través de conexiones de Internet

Información del reporte:

Para citar este reporte técnico:

Martínez Quinto, M. (2025). Comunicación IPv4 segura entre áreas universitarias a través de conexiones de Internet. *Cuadernos Técnicos Universitarios de la DGTIC, 3* (3) páginas(108 - 121).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125

Marcial Martínez Quinto
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
mmarcial@unam.mx
ORCID: 0009-0006-0242-8897

Resumen

Las áreas universitarias cuentan con el acceso a Internet y a RedUNAM a través de enlaces contratados a proveedores de servicios de Internet. Este esquema de red ofrece la conexión directa al campus de Ciudad Universitaria con enlaces dedicados privados (*LAN-to-LAN* y de red privada virtual empresarial). Sin embargo, al presentarse una falla en esas conexiones directas, la comunicación de las áreas universitarias se ve interrumpida, ya que se pierde el servicio de DNS y de recursos de RedUNAM, por lo que la afectación en algunos sitios es prácticamente total. La mitigación del impacto de esos incidentes se realiza de manera manual con la intervención del personal de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación a través del área responsable de velar por la continuidad de la comunicación hacia y desde las áreas universitarias foráneas a Ciudad Universitaria. La necesidad de tener un esquema de red automatizado, para que dicha mitigación no sea manual y se pierdan valiosos minutos en el restablecimiento de la comunicación, dio como origen la elaboración de una alternativa de conexión con los mismos recursos de operación actuales, de forma que, a pesar de que se presenten fallas en cualquier hora del día, los cambios automáticos del tráfico no sean percibidos por los usuarios. Una VPN, construida sobre los enlaces de Internet que brinde seguridad a la información intercambiada, es la solución propuesta en este reporte técnico.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 109 - 121

Palabras clave:

Seguridad, túneles, GRE, IPSec, enlaces a Internet.

Abstract

University campi have access to the Internet and RedUNAM through links contracted with Internet service providers. This network scheme offers direct connection to the Ciudad Universitaria campus with dedicated private links (LAN-to-LAN and enterprise virtual private network). However, if these direct connections fail, communication between university campi is interrupted, as DNS service and RedUNAM resources are lost, resulting in almost complete outage in some locations. The impact of these incidents is mitigated manually with the intervention of staff from the General Directorate of Computing and Information and Communication Technologies, through the area responsible for ensuring the continuity of communication to and from university campi outside Ciudad Universitaria. The need for an automated network scheme to avoid manual mitigation, which would waste valuable time restoring communication, led to the development of an alternative connection using the same current operating resources. This would ensure that, even if failures occur at any time of day, users would not notice the automatic traffic changes. A VPN built over Internet links that provides security for the information exchanged is the solution proposed in this technical report.

Keywords:

Security, tunnels, GRE, IPSec, Internet links.

1. INTRODUCCIÓN

De acuerdo con el manual de organización de la Dirección General de Cómputo de Tecnologías de Información y Comunicación (DGTIC) (Universidad Nacional Autónoma de México [UNAM], 2024), dos de las funciones del Departamento de Monitoreo de DGTIC (NOC RedUNAM) son: monitorear la operación de la infraestructura de conexión de RedUNAM y vigilar su funcionamiento dentro del marco técnico de los contratos correspondientes, en las áreas universitarias de la Zona Metropolitana y del interior de la república (p. 65).

Las conexiones que sirven para comunicar a las áreas universitarias foráneas al Campus Ciudad Universitaria (CU) con la RedUNAM en Ciudad Universitaria son enlaces privados de uso exclusivo para la entidad o dependencia. Estos últimos pueden ser *LAN-to-LAN* o un servicio de red privada virtual empresarial con infraestructura compartida de forma segura sin que el tráfico de cada cliente se vea entre sí. También hay enlaces de Internet que están destinados para acceder a ese recurso, ya sea con fin comercial o para llegar a contenido académico de otras instituciones de educación e investigación. Como lo menciona Tanenbaum (2011), este tipo de conexiones son llamadas WAN (*Wide Area Network*), debido a que interconectan nodos situados en distancias largas, comúnmente a nivel regional, dentro de un país o incluso a través de continentes (p. 23); además, son contratadas a través de los procesos de adquisición o de renta de servicios con base en la legislación universitaria vigente.

El esquema de comunicación en la WAN de RedUNAM de las áreas universitarias foráneas al Campus CU tiene el principal reto de que, al fallar el enlace *LAN-to-LAN* o de red privada virtual que conecta a RedUNAM, se pierde el acceso al servicio de DNS y a los propios recursos de la Universidad. Si bien se

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 110 - 121

puede hacer el enrutamiento del tráfico a través de las conexiones de Internet para que así recobren su conectividad a RedUNAM en Campus CU, no es de forma automatizada, por lo que se pierde valioso tiempo mientras se hace ese cambio manualmente, sin mencionar que el tráfico queda expuesto a las vulnerabilidades existentes en Internet.

En lo que respecta a la comunicación a Internet, debido a que la UNAM cuenta con su propio direccionamiento en las áreas universitarias donde hay enlaces gestionados por el NOC RedUNAM, el intercambio de información con el proveedor de servicios de Internet (ISP por sus siglas en inglés), se hace a través del protocolo BGP con las redes locales (LAN por sus siglas en inglés) de longitud de prefijo de 24 bits para IPv4, mientras que el tráfico de las redes locales con longitud de prefijo mayor (que significa una menor cantidad de nodos disponibles por subred), transita por los enlaces de conexión a RedUNAM al Campus CU (LAN-to-LAN y de red privada virtual empresarial). Por convención entre las organizaciones de Internet, la longitud de prefijo de 24 bits para IPv4 es la más pequeña para propagarse a través de los ISP (Amazon, s.f.), con lo que se busca cumplir las recomendaciones del Grupo de Trabajo de Ingeniería de Internet (IETF por sus siglas en inglés) para obtener el beneficio de una tabla de enrutamiento reducida de redes publicadas en Internet (IETF, 1993).

En el NOC RedUNAM, desde 2022, se ha buscado brindar una alternativa de comunicación automatizada con los recursos actualmente en operación, como lo son los enlaces de Internet que ya están en servicio en las áreas universitarias, de las cuales el personal de DGTIC gestiona su infraestructura y funcionamiento. Así, en escenarios de incidentes de falla de los enlaces de Internet contratados por la UNAM, cuando al menos uno de ellos esté operando, se aprovecha el mayor ancho de banda que hay en esas conexiones y la infraestructura de red de la que se dispone.

2. METODOLOGÍA

La infraestructura actual, que soporta las conexiones WAN de RedUNAM, es, en su gran mayoría, Cisco, por lo que el diseño se basó en los sistemas operativos de este fabricante. Asimismo, el protocolo de enrutamiento interno (IGP por sus siglas en inglés) en RedUNAM es OSPF, por lo que también se consideró en el diseño.

Mediante la *suite* o conjunto de protocolos de IPSec (*Internet Protocol Security*), se puede establecer una conexión segura a través de la red pública de Internet, cifrando el tráfico para evitar que pueda ser visto por terceros que no son los destinatarios del mensaje que se quiere transmitir. Gracias a que es un estándar, tal como lo apunta Aparicio-Izurieta (2022), es soportado por la mayoría de los fabricantes, brindando autenticación, confidencialidad e integridad de la información (pp. 981-982), por lo que se consideró como parte de la solución de VPN implementada.

Un túnel GRE (*Generic Routing Encapsulation*) funge como vía de comunicación virtual entre dos dispositivos que soporten la encapsulación. Así, el mensaje IP original es encapsulado dentro de un paquete GRE, que a su vez es encapsulado en otro paquete IP para su enrutamiento (IETF, 1994a). De esta manera, el mensaje original está dentro de otro paquete IP que tiene el direccionamiento enrutable en Internet, de forma que la conexión entre los dos extremos simula ser directa, mientras la red de en medio sirve de transporte o tránsito. En la solución de VPN propuesta e implementada, la red de tránsito es Internet.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 111 - 121

La solución propuesta es el establecimiento de una red privada virtual (VPN por sus siglas en inglés) que consiste en una conexión de punto a punto; ésta simula una conexión directa entre los dos nodos que se comunican, pero funciona sobre un túnel GRE construido sobre una red de TCP/IP, que, en este caso, es la red de Internet. De acuerdo con De Almeida (2024), IPSec es el estándar de seguridad con la estructura más completa usado en VPN, por lo que, con ese conjunto de protocolos, se asegura que los mensajes serán conocidos sólo por los dispositivos que lo tengan habilitado con los parámetros previamente acordados (p. 4).

Adicional a lo anterior, con la configuración de una traducción de direcciones de red (NAT por sus siglas en inglés), se logra que el tráfico de todas las LAN de las áreas universitarias salgan a Internet y a RedUNAM, utilizando las direcciones IP de los ISP con las que son enumerados los enlaces de Internet y que son conocidas globalmente (IETF, 1994b). De esta forma, se supera la limitante por la convención de proveedores de Internet para que las redes locales con máscara mayor a 24 bits no se vean afectadas por las fallas de los enlaces a RedUNAM (LAN-to-LAN y red privada virtual empresarial).

2.1 DISEÑO

El diseño se hizo primero sobre una maqueta elaborada con el software GNS3 que permite emular los sistemas operativos de los *routers* Cisco, con lo que se evitó hacer pruebas desde cero en equipos en producción. La maqueta puede realizarse con los sistemas operativos soportados por defecto, como los modelos 7200 y dispositivos servidores o computadoras personales que forman parte del propio GNS3 para hacer las pruebas necesarias, tal como lo menciona Salman (2017) en sus pruebas con esa herramienta (p.857).

2.2 CONFIGURACIÓN

Para hacer la configuración, primero se elaboraron los *scripts* en un archivo de texto plano (TXT) antes de aplicarlos a los equipos *routers*.

Para configurar IPSec, es preciso determinar si operará en modo transporte o en modo túnel. Como nos recuerda De Almeida (2024), la diferencia es que el modo transporte se utiliza ampliamente en estructuras donde ya hay implementación de IPSec previa. En cambio, el modo túnel es empleado grandemente en estructuras donde no se ha implementado IPSec, tal es el caso de Internet (Andreoli, 2008, como se citó en De Almeida, 2024, pp. 6-7). Técnicamente, el mensaje original es cifrado en su totalidad en modo túnel, incluido el direccionamiento IP, mientras que, en modo transporte, sólo es la parte del mensaje que corresponde a la información que desea comunicarse. En el caso de la solución propuesta, como lo menciona Aparicio-Izurieta (2022), se usó el modo túnel, que es el método de operación más común cuando se utilizan *routers* que se encargan de procesar el tráfico con IPSec, quedando los equipos de las redes locales y sus aplicaciones sin la necesidad de implementar seguridad (p. 985). Esta forma de implementación de una VPN con IPSec es llamada *Site-to-Site*.

De acuerdo con las recomendaciones de Hadood (2024), el siguiente procedimiento es una buena práctica para establecer una VPN *Site-to-Site* en equipos Cisco:

Definir las credenciales ISAKMP para el intercambio de llaves.

Definir las credenciales de IPSec para el intercambio de datos o información.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 112 - 121

Definir el tráfico de interés para el cifrado a través de una *access-list*.

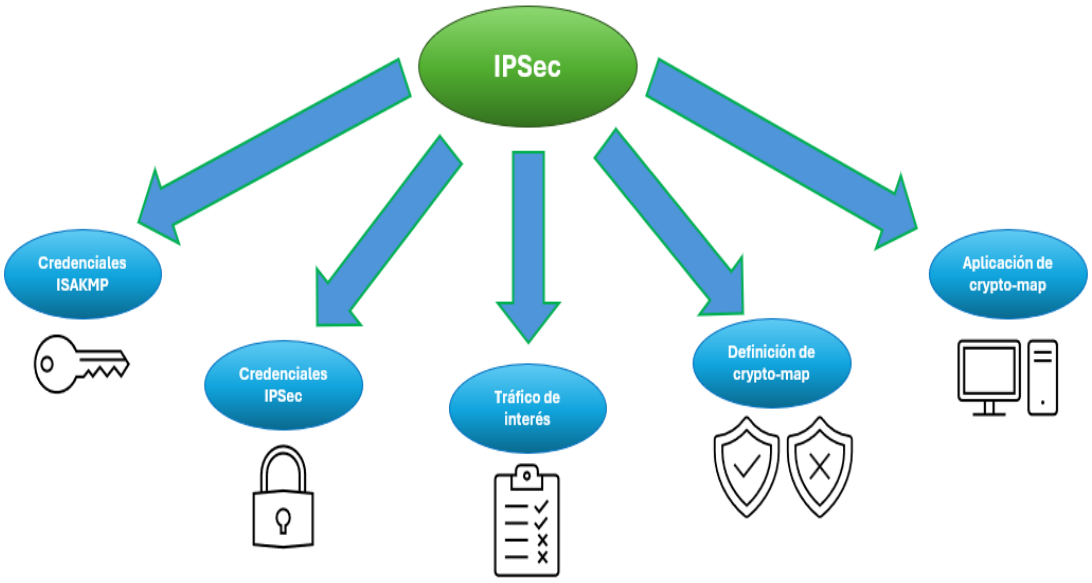
Hacer el *mapping* de todas las credenciales de la VPN en un *crypto map*.

Aplicar el *crypto map* a una interfaz (p. 2305).

Gráficamente, se pueden ver, en la Figura 1, los elementos utilizados para establecer IPSec en la solución propuesta.

Figura 1

Elementos para la implementación de IPSec



El procedimiento que se siguió para la implementación de la VPN con IPSec y túneles GRE se puede examinar con detenimiento en el Anexo A de este documento.

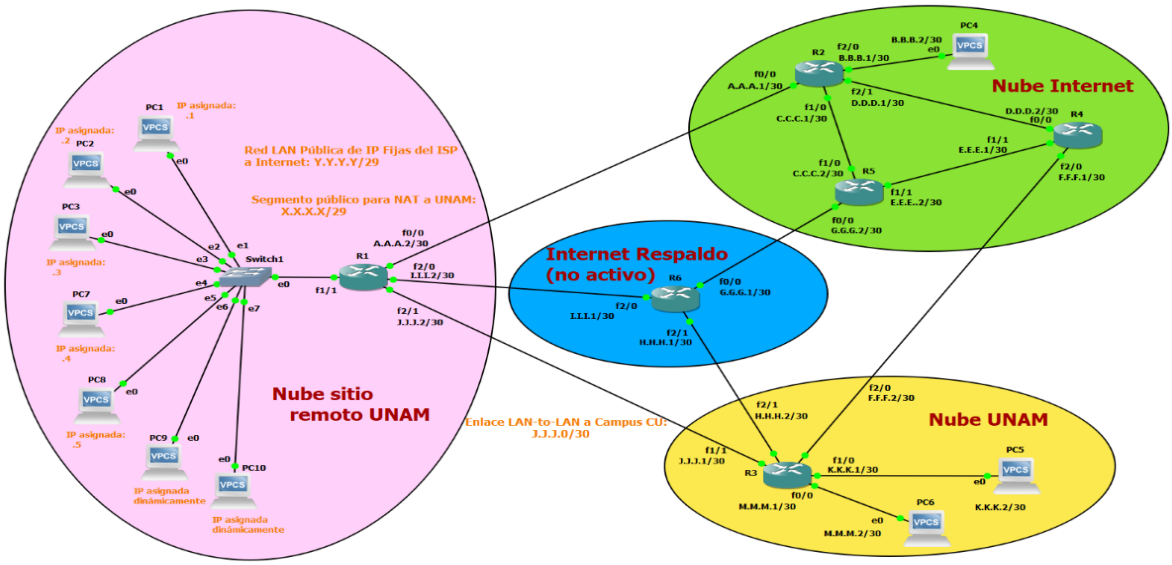
2.3 PRUEBAS

Las pruebas se llevaron a cabo primeramente en una maqueta elaborada en la herramienta de software GNS3, siendo ésta la opción ideal, considerando que fue el primer intento en revisar la factibilidad de la infraestructura actual de RedUNAM en este nuevo paradigma de comunicación. En la Figura 2 se puede apreciar la topología utilizada.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 Vol. 3, Núm. 3. julio-septiembre 2025, págs. 113 - 121

Figura 2

Topología de la maqueta utilizada para las pruebas de la VPN (túneles GRE + IPSec) en la herramienta GNS3



Nota. Por confidencialidad, el direccionamiento IP empleado fue cambiado, pero puede sustituirse por cualquier otro para su adaptación en entornos diferentes. En esta figura, la parte correspondiente al Internet Respaldo tiene la acotación "(no activo)", ya que no siempre hay dos enlaces de Internet en los sitios UNAM; dependerá si aplica esta segunda conexión en cada área universitaria.

Las pruebas en la maqueta constaron de la validación de conectividad entre el sitio remoto y el sitio central, pasando a través de las conexiones de Internet disponibles en dicho sitio remoto. Las verificaciones se llevaron a cabo con las utilidades *traceroute* para corroborar que las trayectorias del tráfico eran correctas (sobre todo si hay dos conexiones de Internet y una de ellas se considera la principal) y *ping* para comprobar que sí había respuesta de los equipos con los que se hizo la comunicación de punta a punta (con una respuesta exitosa de *ping*).

Una vez que se obtuvieron los resultados de comunicación IP satisfactorios, el siguiente paso fue implementarlos en escenarios en producción, con los riesgos que esto conlleva, ya que, si bien hubo resultados correctos a nivel IP, la prueba contundente siempre es a nivel de aplicación.

2.4 IMPLEMENTACIÓN

Con las pruebas satisfactorias en software, lo consecuente fue determinar los sitios para cubrir las áreas universitarias que tienen los diferentes tipos de enlaces contratados para conectarse a RedUNAM. Los nodos seleccionados por cumplir con los requisitos necesarios para su implementación y por la disposición para participar por parte de sus responsables de red fueron los siguientes:

- Un plantel de nivel bachillerato en CDMX que tiene un enlace *LAN-to-LAN* y un enlace de Internet,

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 114 - 121

además de redes locales con máscara igual y mayor a 24 bits.

- Una sede de investigación en el interior de la república que tiene un enlace de red privada virtual empresarial y un enlace de Internet, además de una red local de máscara de 24 bits y con el servicio de telefonía institucional.
- Una facultad en la Zona Metropolitana de CDMX que tiene un enlace *LAN-to-LAN* y un enlace de Internet, además de redes locales con máscara igual y mayor a 24 bits.

Las pruebas de concepto se desarrollaron con la solicitud previa y posterior a la confirmación de los responsables de red de las áreas universitarias involucradas, para que, en caso de una afectación sensible, se contara con un espacio de tiempo que permitiera regresar al estado de operación anterior a la ejecución del cambio. Siempre hubo retroalimentación directa con los responsables de red de esas áreas universitarias, verificando su acceso a las aplicaciones de RedUNAM e Internet.

3. RESULTADOS

En los tres sitios fue satisfactoria la implementación, obteniendo la comunicación correcta a Internet, mientras que la comunicación a RedUNAM se logró que fuera mediante de la VPN construida sobre sus enlaces de Internet y utilizando los túneles GRE protegidos con IPSec.

Con pruebas de utilidades como trazados de ruta y pings, así como con las pruebas de aplicaciones validadas por los responsables de red y sus usuarios, como lo son vía web y aplicaciones móviles y de computadora de escritorio, se pudo confirmar el correcto acceso a Internet a través del NAT (redes LAN con máscaras de red mayores a 24 bits) o directamente (redes LAN con máscaras de red de 24 bits), mientras que, a RedUNAM, fue mediante la VPN-UNAM de túneles GRE con IPSec (para todas las redes LAN). Para lograrlo, se cambió el tamaño del paquete IP, evitando la fragmentación; este punto se aborda mejor en el Anexo A.

Sin embargo, se encontraron fallas que contribuyeron a la mejora de la atención de incidentes que se presentan en RedUNAM. El primer error fue que, debido al NAT, al enmascarar las IP UNAM originales, ya no pueden ser accedidas desde Internet, como con una conexión remota de SSH. La respuesta es retirar de las reglas del NAT, puntualmente de las listas de acceso, las IP específicas que deben ser vistas con IP UNAM desde Internet. Adicionalmente, con el NAT, pueden requerirse muchas traducciones de IP para enmascarar el tráfico, por lo que, al llegar a un límite que depende del *router*, su licenciamiento y hardware, pueden presentarse fallas en el acceso a Internet de las redes locales con máscara mayor a 24 bits. Para resolver este problema, es necesario configurar el NAT en modo de *Carrier Grade*, es decir, darle al proceso del NAT más memoria, retirando información que no es indispensable para su funcionamiento, tal como lo recomienda el fabricante (Cisco, 2016).

Otro problema fue que, cuando hay una falla en los enlaces LAN-to-LAN e Internet, se pueden presentar *loops* que impiden que se logre la comunicación entre las áreas universitarias y el Campus CU, debido a que se genera un comportamiento inesperado con el protocolo OSPF. Esto se corrige reiniciando el proceso de OSPF en los *routers* de los sitios remotos.

Estas problemáticas ya fueron incorporadas al procedimiento para la atención de incidentes de la VPN-UNAM (túneles GRE con IPSec), que sirve para resolver fallas en ese esquema de conexión a RedUNAM.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 115 - 121

Otro hallazgo de gran importancia es que se identificó la necesidad de licenciamiento para que el equipo *router* haga el cifrado del tráfico, de acuerdo con el *throughput* soportado por el dispositivo y con el ancho de banda utilizado sólo para la VPN. Esta consideración depende de cada fabricante y de su línea de licencias para ese propósito. En los tres sitios, se pudo hacer la implementación en un período de licencia que, si bien no tiene soporte de mantenimiento y tiene una limitación en la cantidad de tráfico a cifrar, operativamente sí está permitida por los *routers*, por lo que se pudo continuar la implementación sin inconvenientes.

Cobró mayor importancia tener un esquema de configuraciones de seguridad que permitiera agregar una capa adicional para proteger tanto a los equipos de red, como al tráfico. Un ejemplo lo fue la plantilla de configuración del NOC RedUNAM, que cuenta con líneas para restringir el acceso al dispositivo de enrutamiento (*router*, *switch* o *firewall*), así como la adopción de buenas prácticas de enrutamiento, como lo es la iniciativa MANRS de la Sociedad de Internet (ISOC por sus siglas en inglés). De esta manera, no sólo hay protección en el tráfico, sino también en los equipos de red.

4. CONCLUSIONES

Es claro que, al tener una variedad de enlaces para conectar las áreas universitarias foráneas a RedUNAM, hay ventajas y desventajas, pero el inconveniente principal es que, al quedar fuera la conexión directa al Campus CU, una falla de este tipo puede resultar catastrófica al ocasionar la intervención manual para el restablecimiento de la comunicación.

La VPN mediante túneles GRE con IPSec representa la respuesta automatizada para que, en caso de incidentes en los enlaces WAN, se mantenga el acceso a RedUNAM en las áreas universitarias que se ven afectadas por la falla de sus enlaces. Incluso, se puede prescindir de las conexiones directas al Campus CU que resultan de alto costo, ya que basta con tener enlaces de Internet para poder construir la VPN-UNAM y así establecer la comunicación de forma segura.

Es de resaltar que se debe considerar el hecho de contratar los enlaces de Internet a distintos proveedores, ya que eso incrementa la probabilidad de mantener el acceso a RedUNAM e Internet, en caso de que algún ISP presente fallas en su red e incluso si entra en un estado de contingencia.

Finalmente, pero no menos importante, el equipo técnico responsable de la atención de incidentes de la VPN debe actualizar sus procedimientos para reducir al máximo las afectaciones por fallas y las soluciones de los problemas que se lleguen a presentar en esta nueva forma de conexión a RedUNAM e Internet.

AGRADECIMIENTOS

Tomo este espacio para agradecer a mi jefe, Hugo Rivera, jefe del Departamento de Monitoreo de DGTIC, por darme la confianza de elaborar esta propuesta y por considerarla para los próximos procesos de adquisición de servicios WAN, ya que, a través de esa oportunidad, siento que he aportado y retribuido a mi Universidad.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 116 - 121

REFERENCIAS

Amazon Web Services Inc. (s.f.). Requirements and quotas. *Why is a /24 the smallest IP range that can be used with BYOIP?* https://repost.aws/articles/ARiVYfeM1dS4STKKhkf7LA_Q/why-is-a-24-the-smallest-ip-range-that-can-be-used-with-byoip

Aparicio-Izurieta, V. V. (2022). Segurança IP segura na Internet (IPSEC). *Sapienza: International Journal of Interdisciplinary Studies, 3(1),* 978–987. https://doi.org/10.51798/sijis.v3i1.278

Cisco Systems Inc. (2016, abril). *IP Addressing: NAT Configuration Guide*. Recuperado el 9 de abril de 2025 de https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16/nat-xe-16-book/iadnat-cgn.html

Cisco Systems Inc. (2020, octubre). *Next Generation Cryptography*. Recuperado el 8 de abril de 2025 https://sec.cloudapps.cisco.com/security/center/resources/next_generation_cryptography

Cisco Systems Inc. (2023, mayo). *Resolve IPv4 Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPsec*. Recuperado el 9 de abril de 2025 de https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html

Cisco Systems Inc. (2024, abril). *Understand IPsec IKEv1 Protocol*. Recuperado el 8 de abril de 2025 de https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protocol.html

Hadood, A. K. M. (2024). Implementation of Site to Site IPsec VPN Tunnel using GNS3 Simulation. *International Journal for Research in Applied Science & Engineering Technology (IJRASET),* 12(11), 2302–2307. https://doi.org/10.22214/ijraset.2024.65635

Internet Engineering Task Force. (IETF, septiembre 1993). *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*. https://www.rfc-editor.org/rfc/rfc1519.html#page-9

Internet Engineering Task Force. (IETF, octubre 1994a). *Generic Routing Encapsulation (GRE)*. https://www.rfc-editor.org/rfc/rfc1701.html

Internet Engineering Task Force. (IETF, mayo 1994b). *The IP Network Address Translator (NAT)*. https://www.rfc-editor.org/rfc/rfc1631.html#page-2

De Almeida, F. M. (2024). *O universo das ciências exatas e da terra: teoria e aplicações 2*. Brasil: Atena Editora.

Salman, F. A. (2017). Implementation of IPsec-VPN Tunneling using GNS3. *Indonesian Journal of Electrical Engineering and Computer Science),* 7(3), 855–860. https://doi.org/10.11591/ijeecs.v7.i3.pp855-860

Tanenbaum, A. S. (2011). *Computer Networks*. Estados Unidos de América: Pearson Education.

The National Cyber Security Centre of United Kingdom (2022, marzo). *Using IPsec to protect data*. https://www.ncsc.gov.uk/pdfs/guidance/using-ipsec-protect-data.pdf

Universidad Nacional Autónoma de México. (2024, abril). Manual de organización de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación. https://www.tic.unam.mx/wp-content/uploads/2024/05/Manual-de-Organizacio%CC%81n-DGTIC-2024.pdf

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 117 - 121

ANEXO A

Para hacer la configuración, primero se elaboraron los *scripts* en un archivo de texto plano (TXT) antes de aplicarlos a los equipos *routers* con los que se reciben los enlaces de red privada virtual empresarial, *LAN-to-LAN* e Internet. Se consideraron las recomendaciones mínimas del fabricante Cisco para el establecimiento de una VPN con túneles GRE más IPSec (Cisco, 2020):

- Cifrado con el algoritmo AES de 128 bits.
- Autenticación con los algoritmos RSA o DSA, ambos de 3072 bits.
- Integridad con el algoritmo SHA de 256 bits.
- Intercambio de llaves con el algoritmo Grupo 15 de 3072 bits de Diffie-Hellman (DH).

Estos parámetros del perfil de IPSec son incluso recomendados por el Centro Nacional de Ciberseguridad del Reino Unido (NCSC por sus siglas en inglés) para proveer seguridad a la transmisión de datos (NCSC, 2022, pp. 7-8), aunque con ciertas reservas que deben ser observadas con detenimiento, dependiendo del contexto de cada implementación.

De acuerdo con las recomendaciones de Hadood (2024), el siguiente procedimiento es una buena práctica para establecer una VPN *Site-to-Site* en equipos Cisco:

1. Definir las credenciales ISAKMP para el intercambio de llaves.
2. Definir las credenciales de IPSec para el intercambio de datos o información.
3. Definir el tráfico de interés para el cifrado a través de una *access-list*.
4. Hacer el *mapping* de todas las credenciales de la VPN en un *crypto map*.
5. Aplicar el *crypto map* a una interfaz (p. 2305).

Para el paso 1, se hace uso del protocolo de asociación de seguridad de Internet y de administración de llaves (ISAKMP por sus siglas en inglés), que sirve para establecer un túnel seguro para la autenticación de dos dispositivos en una primera fase, mientras que, en una fase 2, se encarga de negociar los parámetros de seguridad (llaves y algoritmos, llamados *Security Associations*) para el cifrado de la información. ISAKMP también es llamado IKE y hay dos versiones disponibles (Cisco, 2024). En esta propuesta, se emplea la versión 1 de IKE y, siguiendo las recomendaciones del fabricante ya mencionadas, la configuración sería similar a la que a continuación se muestra:

```
!
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 15
!
crypto isakmp key LLAVE_PARA_AUTENTICACIÓN address DIRECCIÓN_IP_ROUTER_REMOTO
!
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 118 - 121

Es importante mencionar que, por motivos de confidencialidad y seguridad, no se ejemplifican configuraciones actualmente en operación, sino que son las mínimas recomendadas por Cisco y el gobierno del Reino Unido.

Para el paso 2, como lo recomienda Salman (2017), se determina un *transformation set* que combina la autenticación y el cifrado de los datos (pp. 857-858). En el caso de esta propuesta, se especifica que será en modo túnel, como se muestra en el siguiente ejemplo, de acuerdo con las recomendaciones mínimas del fabricante Cisco:

```
!
crypto ipsec transform-set NOMBRE_DE_TRANSFORMATION_SET esp-aes esp-sha256-hmac
 mode tunnel
!
```

Para el paso 3 es necesario determinar las reglas que permitan la selección del tráfico que se desea hacer pasar por el túnel, que, en esta propuesta, es el tráfico destinado a comunicarse en RedUNAM, mientras que el resto del tráfico es el que debe enrutarse a Internet. Debido a que la idea es conectar el tráfico mediante el protocolo de enrutamiento OSPF con el túnel VPN simulando una conexión directa, se utiliza la tabla de enrutamiento *default* para que el camino hacia RedUNAM se elija por OSPF (hacia el Campus CU) y el camino a Internet se vea por el protocolo BGP (hacia los proveedores de Internet). Ello significa que, para esta propuesta, no es necesario configurar una *access-list* para seleccionar el tráfico que debe pasar por la VPN, ya que de eso se encargará el enrutamiento por sí mismo.

Si bien no es necesaria la lista de acceso para seleccionar el tráfico que transitará por el túnel VPN, sí se emplea una para que las redes locales con máscaras de red mayores a 24 bits utilicen un NAT con las direcciones IP de los ISP, de forma que sí tengan acceso a Internet, sorteando la limitación de la propagación de redes con máscara de hasta 24 bits en Internet. En esta propuesta de VPN, las dos técnicas sencillas son negar el tráfico que sea destinado a RedUNAM y permitir el tráfico de las redes locales con máscaras mayores a 24 bits que vayan a cualquier destino. La configuración ejemplo es la siguiente:

```
!
ip access-list extended LISTA_DE_ACCESO_PARA_EL_NAT_A_INTERNET
 deny   ip any X.X.X.X X.X.X.X
 deny   ip any Y.Y.Y.Y Y.Y.Y.Y
 permit ip L.L.L.L L.L.L.L any
 permit ip M.M.M.M M.M.M.M any
 permit ip N.N.N.N N.N.N.N any
!
```

En donde X.X.X.X y Y.Y.Y.Y son los segmentos de red y su *wildcard* a la que no queremos llegar para salir a Internet, y L.L.L.L, M.M.M.M y N.N.N.N son las redes locales y sus *wildcards* con máscara de red mayor a 24 bits que requieren acceder a Internet mediante el NAT.

Para concluir con la definición de las reglas del NAT, se especifica la interfaz del *router* que conecta el enlace de Internet como salida para el NAT, además de que con un *route-map* se indica que el tráfico, que sea seleccionado por la lista de acceso definida previamente, se dirija por las interfaces de salida del NAT, para que así el tráfico sea enmascarado con la IP del proveedor del enlace:

```
!
interface GigabitEthernet0/1
 ip nat outside
!
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 119 - 121

```
route-map NAT_A_INTERNET permit 10
 match ip address LISTA_DE_ACCESO_PARA_EL_NAT_A_INTERNET
 match interface GigabitEthernet0/1
!
ip nat inside source route-map NAT_A_INTERNET interface GigabitEthernet0/1 overload
!
```

Para el paso 4, se debe hacer el *mapping* de las credenciales o parámetros de la VPN en un elemento que se llama *crypto map*, pero, en el caso de esta propuesta de VPN que emplea el modo túnel de IPSec, se usa un perfil con los mismos parámetros del *transform set* previamente definido, para que posteriormente, dicho perfil sea aplicado a las interfaces que se necesiten en el paso siguiente. Las configuraciones básicas recomendadas son las que a continuación se muestran:

```
!
crypto ipsec profile PERFIL_IPSEC_PARA_CIFRADO
 set transform-set NOMBRE_DE_TRANSFORMATION_SET
!
```

Para el último paso 5, se aplica el *crypto map* a las interfaces que sean objeto de la VPN, aunque, en el caso de esta propuesta, se trata del perfil definido previamente. Como se mencionó al principio, la idea es que se emplee un túnel GRE para discernir la comunicación a RedUNAM de la que es dirigida a Internet. Primeramente, se configura una interfaz túnel en cada *router* de los extremos, considerando las direcciones IP de los proveedores de Internet que reciben esos enlaces y que se utilizarán como la red de transporte sobre la que se construye el túnel, además del direccionamiento IP que enumerará ambas puntas para el establecimiento del intercambio de tráfico mediante el protocolo OSPF. Para evitar intermitencia en el establecimiento de la VPN, se debe configurar una ruta estática para alcanzar la IP destino con la que se construye el túnel. Las configuraciones siguientes ejemplifican este paso:

Equipo *router* remoto

```
!
ip route U.U.U.U U.U.U.U GigabitEthernet0/0 I.I.I.1 name IP_TUNNEL_A_SITIO_CENTRAL
!
interface Tunnel1
 description TUNNEL_A_SITIO_CENTRAL
 ip address Z.Z.Z.2 Z.Z.Z.Z
 tunnel source I.I.I.2
 tunnel destination U.U.U.2
!
```

Equipo *router* central

```
!
ip route I.I.I.I I.I.I.I GigabitEthernet0/0 U.U.U.1 name IP_TUNNEL_A_SITIO_REMOTO
!
interface Tunnel1
 description TUNNEL_A_SITIO_REMOTO
 ip address Z.Z.Z.1 Z.Z.Z.Z
 tunnel source U.U.U.2
 tunnel destination I.I.I.2
!
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 120 - 121

En donde I.I.I.I y U.U.U.U son las IP y sus máscaras de red del enlace de Internet en cada extremo de la comunicación sobre los cuales se construye el túnel VPN, mientras que Z.Z.Z.Z es el segmento de red de interconexión entre los dos *routers* de cada punta para el intercambio de tráfico a través del protocolo OSPF. La configuración del protocolo OSPF se ejemplifica a continuación:

```
!
router ospf 1
 network Z.Z.Z.Z Z.Z.Z.Z area 0.0.0.0
!
```

Finalmente, se aplica el perfil de IPSec a las interfaces túneles para que se cifre el tráfico que va destinado, en el caso de esta propuesta de VPN, a RedUNAM:

Equipo *router* remoto

```
!
interface Tunnel1
 description TUNNEL_A_SITIO_CENTRAL
 tunnel protection ipsec profile PERFIL_IPSEC_PARA_CIFRADO
!
```

Equipo *router* central

```
!
interface Tunnel1
 description TUNNEL_A_SITIO_REMOTO
 tunnel protection ipsec profile PERFIL_IPSEC_PARA_CIFRADO
!
```

Como paso extra y último de esta propuesta de VPN, se aplica el NAT en las interfaces del *router* de ambos extremos que tengan las redes locales con máscaras mayores a 24 bits para que salgan a Internet con las IP de los proveedores de esos enlaces:

```
!
interface INTERFAZ_LAN_1
 ip tcp adjust-mss 1370
 ip nat inside
!
```

Es importante no olvidar que se debe configurar el ajuste del tamaño del paquete, ya que, conforme se añaden protocolos y sus encabezados, como lo son GRE y el propio IPSec, se incrementa su tamaño, por lo que, para evitar la fragmentación que ocasiona problemas en las aplicaciones, el fabricante Cisco recomienda hacer modificaciones del tamaño de la MTU en la interfaz física, habilitar la negociación del tamaño de MTU automático en los túneles o aplicar directamente el tamaño en las interfaces de los *routers* donde se origine el tráfico que cruzará por la VPN (Cisco, 2023). En el caso de esta propuesta, se determinó que el número de bytes es de 1370, una vez hecho el análisis del tamaño de los encabezados y pruebas con los equipos de cómputo desde las redes locales de algunos sitios para acceder a las aplicaciones de Internet y RedUNAM.

Para finalizar, es recomendable agregar una capa de seguridad al equipo que tenga la VPN configurada, en este caso, un *router*. Obviamos que debe existir un usuario y contraseña exclusivos para acceder

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 121 - 121

al dispositivo, ya sea configurado localmente o mediante un servidor que centralice ese control. La restricción de acceso al equipo se puede implementar de forma sencilla con una lista de control de acceso para permitir sólo a las IP puntuales que deberán tener la autorización para ingresar al equipo:

```
!
username usuario_autorizado secret contrasenia_usuario_autorizado
!
ip access-list standard ACL_ACCESO_REMOTO
 permit X.X.X.X 0.0.0.0
 permit Y.Y.Y.Y 0.0.0.0
 permit Z.Z.Z.Z 0.0.0.0
!
line con 0
 login local
 access-class ACL_ACCESO_REMOTO in
!
line vty 0 4
 login local
 access-class ACL_ACCESO_REMOTO in
!
```

También puede considerarse la implementación de la iniciativa MANRS de la ISOC para tratar de lograr un enrutamiento más seguro en Internet. No se profundiza en esta capa adicional de seguridad, ya que escapa del ámbito principal y de la propuesta de solución de VPN de este reporte técnico.

CUADERNOS TÉCNICOS UNIVERSITARIOS DE LA DGTIC

ISSN-e: 3061-8096

DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN