Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), septiembre-octubre 2024,
Volumen 8, Número 5.

https://doi.org/10.37811/cl_rcm.v8i5

IMPACTO DE LA IMPLEMENTACIÓN DE REDES PRIVADAS VIRTUALES PARA LA INTERCONEXIÓN DE CAMPUS UNIVERSITARIOS EN LA UNIVERSIDAD ESTATAL AMAZÓNICA

IMPACT OF VIRTUAL PRIVATE NETWORK IMPLEMENTATION FOR CAMPUS INTERCONNECTION AT UNIVERSITY ESTATAL AMAZONICA

Edwin Gustavo Fernández Sánchez
Universidad Estatal Amazónica, Ecuador

Alberto Alexander Aldás Villacreces
Universidad Estatal Amazónica, Ecuador

Verónica Villarreal Morales
Universidad Estatal Amazónica, Ecuador

Katherine Estefania Coro Villarreal
Universidad Estatal Amazónica, Ecuador

DOI: https://doi.org/10.37811/cl_rcm.v8i5.14759

Impacto de la Implementación de Redes Privadas Virtuales para la Interconexión de Campus Universitarios en la Universidad Estatal Amazónica

Edwin Gustavo Fernández Sánchez[1]
gfernandez@uea.edu.ec
https://orcid.org/0000-0002-2613-4774
Universidad Estatal Amazónica
Provincia de Pastaza- Puyo
Ecuador

Alberto Alexander Aldás Villacreces
aaldas@uea.edu.ec
https://orcid.org/0009-0004-0430-2839
Universidad Estatal Amazónica
Provincia de Pastaza- Puyo
Ecuador

Verónica Villarreal Morales
vvillarreal@uea.edu.ec
https://orcid.org/0000-0002-6401-3404
Universidad Estatal Amazónica
Provincia de Pastaza- Puyo
Ecuador

Katherine Estefania Coro Villarreal
ke.corov@uea.edu.ec
https://orcid.org/0009-0009-7667-7767
Universidad Estatal Amazónica
Provincia de Pastaza- Puyo
Ecuador

RESUMEN

El presente documento analiza el impacto de la implementación de Redes Privadas Virtuales (VPN) para la interconexión de campus universitarios en la Universidad Estatal Amazónica (UEA). Justificada por la dispersión geográfica y las limitaciones económicas, la investigación tuvo como objetivo evaluar cómo las VPNs mejoran la seguridad, disponibilidad y gestión de la infraestructura de TI. Se empleó una metodología mixta, combinando métodos cuantitativos y cualitativos, con un enfoque explicativo que abarcó la interconexión mediante VPNs, alta disponibilidad y monitoreo continuo. Los resultados relevantes mostraron una mejora significativa en la disponibilidad y seguridad de los servicios en las sedes de Pangui y Lago Agrio, mientras que la sede de CEIPA enfrentó desafíos debido a factores externos como la estabilidad del suministro eléctrico. La discusión de los hallazgos evidenció que, aunque el impacto ha sido positivo en general, aún existen brechas que deben cerrarse mediante un mantenimiento más riguroso, seguimiento continuo y la implementación de fuentes de energía redundantes. Las conclusiones destacan que la combinación de VPNs y tecnologías de alta disponibilidad es efectiva para optimizar la gestión de la infraestructura de TI, pero es fundamental abordar factores adicionales para lograr una interconexión completamente resiliente y segura en todas las sedes de la UEA.

Palabras clave: ciberseguridad, vpn; alta disponibilidad, infraestructura, interconexión

[1] Autor principal
Correspondencia: gfernandez@uea.edu.ec

Impact of Virtual Private Network Implementation for Campus Interconnection at University Estatal Amazonica

ABSTRACT

This document analyzes the impact of implementing Virtual Private Networks (VPNs) for interconnecting university campuses at the Universidad Estatal Amazónica (UEA). Justified by geographical dispersion and economic limitations, the study aimed to evaluate how VPNs enhance the security, availability, and management of the IT infrastructure. A mixed methodology was employed, combining quantitative and qualitative methods, with an explanatory approach encompassing VPN interconnection, high availability, and continuous monitoring. Relevant results demonstrated a significant improvement in the availability and security of services in the Pangui and Lago Agrio campuses, while the CEIPA campus faced challenges due to external factors such as electrical supply stability. The discussion of findings revealed that, although the overall impact has been positive, gaps still exist that need to be addressed through more rigorous maintenance, continuous monitoring, and the implementation of redundant energy sources. The conclusions highlight that the combination of VPNs and high availability technologies is effective in optimizing IT infrastructure management, but it is essential to address additional factors to achieve a fully resilient and secure interconnection across all UEA campuses.

***Keywords*:** cybersecurity, vpn, high availability, infrastructure, interconnection

Artículo recibido 30 octubre 2024
Aceptado para publicación: 20 noviembre 2024

INTRODUCCIÓN

La Universidad Estatal Amazónica (UEA), con sede en la ciudad de Puyo (provincia de Pastaza), es una institución pública ecuatoriana dedicada a la educación superior, cuya misión es contribuir activamente al desarrollo sostenible de la región amazónica a través de la formación de profesionales y la investigación aplicada. La universidad cuenta con diversos campus distribuidos en zonas geográficamente apartadas, como el Centro Experimental de Investigación y Producción Amazónica (CEIPA), en la provincia de Napo, y dos sedes académicas en Lago Agrio (Sucumbíos) y El Pangui (Zamora Chinchipe).

La interconexión de los campus y sedes académicas de la UEA enfrenta importantes desafíos tecnológicos debido a la dispersión geográfica y la limitación de recursos económicos. Los avances en tecnología de la información y la comunicación (TIC) han permitido a muchas instituciones de educación superior implementar redes privadas virtuales (VPN) para garantizar la seguridad de la información y acortar las distancias entre sus sedes. Diversos estudios han abordado el uso de VPNs para garantizar la confidencialidad, integridad y disponibilidad de los datos en redes distribuidas, destacando su capacidad para asegurar infraestructuras críticas como las universidades y centros de investigación.

En el caso de la UEA, el uso de tecnologías de ciberseguridad se ha vuelto una prioridad, especialmente para cumplir con normativas internacionales como la ISO 27.001 (relacionada con la gestión de la seguridad de la información) y la ISO 38.500 (organization), así como con leyes nacionales como la Ley de Protección de Datos Personales de Ecuador y el Esquema Gubernamental de Seguridad de la Información.

La interconexión segura de la infraestructura de TI en la UEA no solo es crucial para garantizar la continuidad de los servicios académicos y administrativos, sino también para cumplir con las normativas de la Seguridad de la Información (Pública, 2013).

Las VPNs permiten a la UEA extender sus redes LAN de manera segura y transparente entre el campus principal y sus sedes, asegurando que la información crítica como la telefonía y la videovigilancia se transmita de manera encriptada, protegiendo la privacidad de los datos y reduciendo la exposición a ciberataques.

Un factor importante que permite garantizar la interconexión es la implementación de tecnologías de alta disponibilidad, que permiten mantener el acceso continuo a internet mediante enlaces redundantes con balanceo de carga y failover en caso de fallos en los proveedores de servicios.

El uso de VPNs y tecnologías de ciberseguridad para la interconexión de redes de universidades no es un concepto nuevo. En investigaciones previas, se ha demostrado que las VPNs pueden ofrecer una solución robusta y económica para garantizar la seguridad en redes distribuidas. Según estudios de (Chinkes, 2015), la implementación de VPNs en instituciones educativas ha permitido no solo reducir costos, sino también mejorar la disponibilidad de los servicios al optimizar la gestión de recursos tecnológicos.

No obstante, uno de los desafíos más relevantes, según (ISACA, 2013) radica en la necesidad de una administración centralizada de los sistemas para garantizar la eficiencia y evitar redundancias operativas, lo cual coincide con los objetivos planteados por la UEA. La integración de soluciones como PFSense, una plataforma de código abierto para la gestión de VPNs y seguridad perimetral, ha demostrado ser una herramienta viable para instituciones que buscan una solución económica y adaptable.

Este artículo pretende analizar los aspectos clave de la interconexión de la infraestructura de TI entre el campus principal de la UEA y sus sedes académicas, enfocándose en ciberseguridad, VPNs y alta disponibilidad. Se estudia cómo estas tecnologías aseguran la transmisión segura de datos entre ubicaciones dispersas, protegiendo información sensible y garantizando la operatividad continua de los servicios críticos. El objetivo es demostrar cómo la implementación de enlaces redundantes y VPNs optimiza la gestión de la infraestructura tecnológica, cumpliendo con normativas de ciberseguridad y asegurando la continuidad operativa.

METODOLOGÍA

Enfoque de la investigación

El enfoque de esta investigación es mixto, combinando métodos cuantitativos y cualitativos para evaluar la evolución, el impacto y la efectividad de la infraestructura de TI en la Universidad Estatal Amazónica (UEA). Se han implementado diversas soluciones tecnológicas a lo largo de los años, y este estudio

busca tanto analizar los resultados numéricos de las mejoras como entender las decisiones estratégicas que las guiaron.

Métodos cuantitativos

El análisis cuantitativo se sustenta en datos recolectados por herramientas de monitoreo como Zabbix, que miden la disponibilidad de los enlaces de internet, el rendimiento de los servidores y el tiempo de inactividad de los servicios críticos. Los indicadores clave son:

- Disponibilidad de enlaces de internet (% de tiempo en línea).
- Alertas generadas por el sistema sobre rendimiento de servidores y redes.
- Tiempo de inactividad de los servicios críticos por mes.

Estos datos son cruciales para demostrar el impacto de la implementación de Redes Privadas Virtuales (VPN) para la interconexión de sedes en la Universidad Estatal Amazónica (UEA) mejorando la seguridad de la infraestructura.

Métodos cualitativos

El enfoque cualitativo se centra en evaluar las decisiones estratégicas a lo largo de la evolución de la infraestructura de TI. Se analiza cómo la UEA ha adaptado sus sistemas en respuesta a las necesidades operativas, normativas internacionales de ciberseguridad y el crecimiento institucional. Se busca explicar por qué se tomaron ciertas decisiones y cómo influyeron en la eficiencia operativa y la seguridad de la infraestructura.

Alcance de la investigación

El alcance es explicativo, ya que se centra en analizar y demostrar cómo la implementación de Redes Privadas Virtuales (VPN) para la interconexión de sedes en la Universidad Estatal Amazónica (UEA) ha optimizado la gestión de la infraestructura de TI en la UEA. El estudio abarca la mejora en la continuidad operativa, la resiliencia y la seguridad de los servicios críticos. Las áreas clave incluyen:

- Interconexión mediante VPN: Evaluación del impacto en la gestión centralizada y la seguridad de los datos.
- Alta disponibilidad y redundancia: Análisis de la implementación de enlaces redundantes con balanceo de carga y failover.

- Monitoreo continuo: Impacto de las herramientas de monitoreo en la detección de fallos y optimización de la infraestructura

Exclusiones y limitaciones

- Exclusión geográfica: La investigación se centra únicamente en las sedes conectadas de la UEA (Puyo, CEIPA, Lago Agrio y El Pangui). No se abordan otras posibles conexiones externas fuera de estas sedes.
- Limitaciones temporales: La investigación analiza el impacto de las implementaciones hasta el año 2024. No se cubren desarrollos futuros más allá de este año.
- Focalización tecnológica: Aunque se mencionarán diversas tecnologías como PFSense, Mikrotik, Zabbix, entre otras, no se realiza un análisis detallado de todas las posibles soluciones tecnológicas disponibles en el mercado, sino que el enfoque está en las tecnologías que se han implementado en la UEA

Criterio de selección de la población y muestra

La población incluye los equipos de comunicación principales de cada sede. Estos equipos son esenciales para la interconexión, el acceso a internet y la gestión de servicios críticos como la telefonía, la videovigilancia y la gestión académica. La muestra está compuesta por los datos recolectados de estos equipos en los últimos dos años, permitiendo medir el rendimiento y la disponibilidad de los servicios. Los datos provienen del sistema de monitoreo continuo Zabbix, que ofrece una visión clara del estado de la infraestructura.

Variables de investigación

Variables cuantitativas

- Disponibilidad de los enlaces de internet (% de tiempo en línea).
- Tiempo de inactividad de los servicios críticos (horas por mes).
- Número de alertas generadas por Zabbix.

Variables Cualitativas

- Efectividad de las decisiones estratégicas en la mejora de la infraestructura.
- Satisfacción del equipo de TI y usuarios respecto a la disponibilidad y seguridad.
- Evolución a lo largo del tiempo de cómo ha ido cambiando la interconexión de las sedes de la UEA

RESULTADOS Y DISCUSIÓN

Evolución de las implementaciones y avances realizados en la interconexión de las sedes a lo largo del tiempo y decisiones estratégicas tomadas

Iteración 1: Implementación inicial de redes locales (2013-2016)

Análisis del problema

Durante esta iteración, la necesidad primordial era proporcionar conectividad a las sedes de CEIPA, Lago Agrio y El Pangui, que hasta ese momento funcionaban de manera independiente sin acceso a una infraestructura de red compartida o gestionada centralmente. El análisis realizado durante este periodo identificó que una red local bien implementada sería la base para interconectar las sedes en el futuro.

Investigación de soluciones

La investigación de tecnologías disponibles para la implementación de redes locales llevó a la conclusión de que las soluciones de código abierto ofrecían la flexibilidad y el bajo costo necesarios para el proyecto.

Se consideraron varias alternativas antes de elegir tecnologías que permitirían una expansión escalonada de la infraestructura sin comprometer la sostenibilidad financiera del proyecto.

Implementación

La solución elegida fue implementar redes locales en cada sede de manera independiente, con el objetivo de mejorar la gestión interna y proporcionar acceso a internet. El proceso incluyó la creación de sistemas de red basados en open source, asegurando que, una vez conectadas las sedes al campus principal, la integración fuese fluida y segura.

Iteración 2: Interconexión mediante VPNs (2015-2016)

Análisis del problema

Con las redes locales establecidas, el siguiente desafío era interconectar las sedes con el campus principal en Puyo para asegurar la gestión remota y garantizar la seguridad en la transmisión de datos. El análisis del problema reveló que, sin una solución de interconexión segura, la universidad no podría centralizar la gestión de sus servicios de TI ni ofrecer soporte técnico adecuado a las sedes remotas.

Investigación de tecnologías VPN

Se evaluaron diferentes opciones para implementar VPNs, y se decidió adoptar una solución de código abierto, Zentyal, que permitiría la creación de una red privada extendida. Esta elección fue el resultado de una investigación que priorizaba soluciones flexibles, seguras y con capacidad de escalabilidad para adaptarse al crecimiento de la UEA.

Implementación y monitoreo

La implementación de VPNs se realizó en un contexto de prueba inicial con la sede de CEIPA y, posteriormente, se extendió a Lago Agrio y El Pangui. Este proceso fue acompañado de un monitoreo continuo para evaluar el rendimiento y asegurar que los datos transmitidos entre las sedes estuvieran protegidos de acuerdo con las normativas de seguridad.

Iteración 3: Migración a PFSense (2018)

Análisis del Problema

A medida que la infraestructura de la UEA crecía, la solución de VPN basada en Zentyal comenzó a mostrar limitaciones en términos de robustez, escalabilidad y seguridad avanzada. El análisis mostró que la creciente demanda de gestión centralizada y las nuevas normativas de ciberseguridad requerían una solución más avanzada que permitiera manejar el aumento del tráfico de red y garantizar la protección de los datos sensibles.

Investigación y evaluación

La investigación realizada en 2018 se centró en identificar una plataforma de seguridad perimetral que pudiera soportar conexiones seguras para varias sedes y cumplir con las exigencias de la ISO 27001 (Security techniques — Information security management systems). Tras evaluar varias alternativas, se eligió PFSense por su flexibilidad, alto nivel de seguridad y capacidad para gestionar múltiples VPNs y conexiones simultáneas con encriptación avanzada.

Implementación

La migración a PFSense fue un proceso estructurado que incluyó pruebas piloto y la configuración avanzada de las nuevas VPNs. Durante este tiempo, se establecieron nuevos protocolos de seguridad para las conexiones de red y se mejoró la gestión perimetral. Este cambio permitió una mayor escalabilidad y preparó la infraestructura para manejar futuros desafíos operativos.

Iteración 4: Implementación de enlaces redundantes (2024)

Análisis del problema

La creciente dependencia de los servicios críticos de TI llevó a la necesidad de garantizar alta disponibilidad en los enlaces de internet. Se identificó que la infraestructura estaba vulnerable ante fallos en el único proveedor de internet en cada sede, lo que podría resultar en interrupciones significativas en los servicios.

Investigación de soluciones de alta disponibilidad

El análisis investigativo se centró en soluciones de redundancia de enlaces y balanceo de carga que garantizaran que los servicios no se interrumpieran en caso de un fallo en uno de los proveedores de internet.

Tras analizar las opciones disponibles en el mercado, se decidió utilizar enlaces redundantes provistos por CEDIA y CNT respectivamente, gestionados con equipos Mikrotik, debido a su capacidad de realizar failover y balanceo de carga de manera eficiente.

Implementación y evaluación

La implementación incluyó la configuración de dos enlaces de internet en cada sede y la integración de equipos Mikrotik para gestionar el balanceo y failover. Esta solución fue probada bajo diferentes escenarios de falla para asegurar que los servicios críticos, como la telefonía y la videovigilancia, no sufrieran interrupciones.

El análisis continuo de los resultados ha demostrado una mejora significativa en la resiliencia y disponibilidad de los servicios de TI.

Resultados Cualitativos

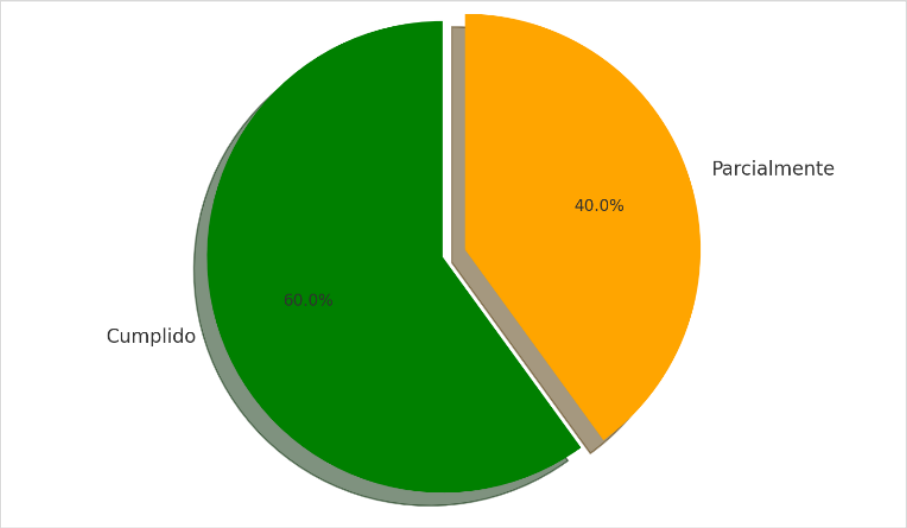
En esta sección se presentan los resultados obtenidos a partir de las variables cualitativas definidas en la metodología, enfocándose en la efectividad de las decisiones estratégicas, la satisfacción del equipo de TI y de los usuarios, así como la evolución de la interconexión de las sedes de la UEA.

Efectividad de las Decisiones Estratégicas en la Mejora de la Infraestructura

Tabla 1. Resultados de Decisiones Estratégicas en cumplimiento de Control ISO 27001

Control ISO 27001	Cumplimiento	Observaciones
Control de acceso perimetral	Cumplido	Se utilizan firewalls y VPNs para proteger el perímetro de la red.
Gestión de incidentes	Parcialmente	El tiempo de respuesta a incidentes ha mejorado, pero aún hay margen para una respuesta más rápida.
Continuidad operativa	Cumplido	Se implementaron enlaces redundantes para asegurar la disponibilidad en caso de fallas.
Evaluación de vulnerabilidades	Parcialmente	No se realizan pruebas de estrés frecuentes para evaluar la seguridad del firewall.
Capacitación del personal de TI	Cumplido	El personal ha recibido capacitación en la gestión de incidentes de seguridad.

Figura 1 | Cumplimento de Controles ISO 27001 para Decisiones Estratégicas

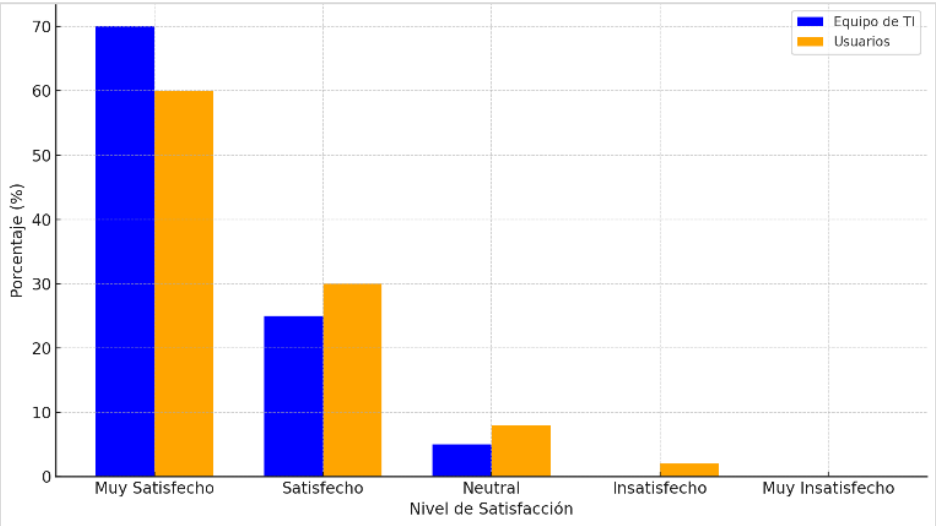


Las decisiones estratégicas implementadas a lo largo de las distintas iteraciones han demostrado una alta efectividad en la mejora de la infraestructura de TI de la UEA. La migración a plataformas más robustas como PFSense permitió una gestión centralizada y segura de las VPN, lo que facilitó la expansión y el mantenimiento de la red interconectada. Además, la implementación de enlaces redundantes en 2024 incrementó significativamente la disponibilidad y resiliencia de los servicios críticos, reduciendo la vulnerabilidad ante fallos de proveedores de internet.

Estas decisiones estratégicas reflejan una alineación con las mejores prácticas en gestión de TI y ciberseguridad, cumpliendo con normativas internacionales como la ISO 27001. La adopción de tecnologías de código abierto y soluciones escalables permitió a la UEA optimizar recursos financieros mientras garantizaba una infraestructura robusta y adaptable a futuras necesidades.

Satisfacción del Equipo de TI y Usuarios respecto a la Disponibilidad y Seguridad

Figura 2 | Satisfacción del Equipo de TI y Usuarios respecto a la Disponibilidad y Seguridad



Las encuestas realizadas al equipo de TI y a los usuarios de las diferentes sedes revelaron un alto nivel de satisfacción con respecto a la disponibilidad y seguridad de los servicios de TI. Los miembros del equipo de TI destacaron la facilidad de gestión centralizada y la capacidad de monitoreo continúo proporcionada por las herramientas implementadas, lo que les permitió responder de manera más eficiente a incidentes y mantener la infraestructura operativa.

Por otro lado, los usuarios finales reportaron una experiencia de conectividad más fluida y segura, con acceso a servicios como videovigilancia, telefonía IP y acceso federado en equipos de escritorio, sin interrupciones significativas. La interconexión eficiente hizo que los usuarios percibieran las sedes como una única entidad cohesiva, mejorando la colaboración y el acceso a recursos académicos y administrativos. La satisfacción tanto del equipo de TI como de los usuarios indica que las soluciones implementadas no solo cumplen con los requisitos técnicos, sino que también aportan valor añadido en términos de usabilidad y confianza en los sistemas de TI. Esto es fundamental para fomentar un entorno académico y administrativo eficiente y seguro, donde la tecnología apoya de manera efectiva las actividades sustantivas de la universidad.

Evolución de la Interconexión de las Sedes de la UEA

A lo largo de las diferentes iteraciones, la interconexión de las sedes de la UEA ha evolucionado de una red local independiente a una infraestructura altamente integrada y segura. Inicialmente, cada sede operaba de manera aislada, lo que limitaba la eficiencia y la capacidad de colaboración entre ellas. La implementación de VPN permitió una conexión segura y centralizada, facilitando la gestión remota y la cohesión de los servicios de TI.

La migración a PFSense y la posterior implementación de enlaces redundantes consolidaron esta evolución, garantizando no solo la seguridad y disponibilidad de los datos, sino también la capacidad de adaptación a futuras expansiones o cambios tecnológicos. Esta evolución ha permitido a la UEA mantener una infraestructura de TI robusta y flexible, alineada con sus objetivos de desarrollo sostenible y crecimiento institucional. La evolución de la interconexión refleja una planificación estratégica efectiva y una capacidad de adaptación a las necesidades cambiantes de la institución. Al centralizar la gestión de TI y asegurar la redundancia en los enlaces de internet, la UEA ha logrado una infraestructura resiliente que soporta tanto las operaciones actuales como las futuras expansiones, asegurando así la continuidad de los servicios académicos y administrativos.

Datos Cualitativos

Tabla 2. Sede Académica El Pangui

Mes-Año	N. Caídas	Duración Total de Caídas (Horas)	Tiempo Operativo Total (Horas)	Disponibilidad (%)
01/09/2023	3	0.49	720	99.93
01/10/2023	1	0.1	720	99.99
01/11/2023	5	0.42	720	99.94
01/12/2023	5	1.52	720	99.79
01/01/2024	3	0.29	720	99.96
01/02/2024	5	3.15	720	99.56
01/03/2024	16	5.4	720	99.25
01/04/2024	49	53.02	720	92.64
01/05/2024	15	15.21	720	97.89
01/06/2024	15	2.91	720	99.6
01/07/2024	15	7.11	720	99.01
01/08/2024	3	5.99	720	99.17
01/09/2024	4	10.24	720	98.58

Tabla 3. Sede Académica Lago Agrío

Mes-Año	N. Caídas	Duración Total de Caídas (Horas)	Tiempo Operativo Total (Horas)	Disponibilidad (%)
01/09/2023	5	0.28	720	99.96
01/10/2023	49	10.32	720	98.57
01/11/2023	31	2.41	720	99.67
01/12/2023	27	16.29	720	97.74
01/01/2024	31	2.17	720	99.7
01/02/2024	20	3.84	720	99.47
01/03/2024	99	18.29	720	97.46
01/04/2024	176	47.3	720	93.43
01/05/2024	117	12.29	720	98.29
01/06/2024	2	0.47	720	99.93
01/07/2024	3	0.11	720	99.98
01/08/2024	3	0.45	720	99.94
01/09/2024	4	70.51	720	90.21

Tabla 4. Centro Experimental de Investigación y Producción Amazónica

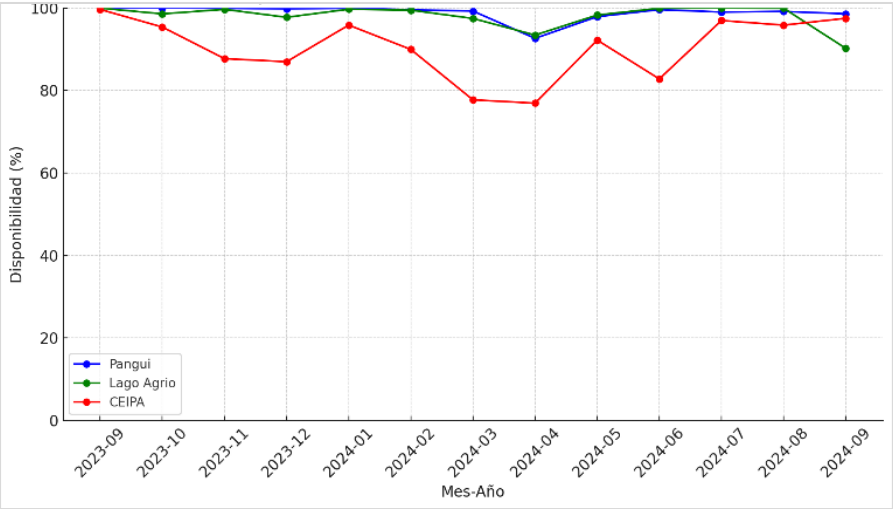
Mes-Año	N Caídas	Duración Total de Caídas (Horas)	Tiempo Operativo Total (Horas)	Disponibilidad (%)
01/09/2023	2	2.6	720	99.64
01/10/2023	28	33.23	720	95.38
01/11/2023	49	88.4	720	87.72
01/12/2023	31	93.8	720	86.97
01/01/2024	14	29.9	720	95.85
01/02/2024	17	72.38	720	89.95
01/03/2024	41	160.34	720	77.73
01/04/2024	37	166.14	720	76.92
01/05/2024	29	56.06	720	92.21
01/06/2024	21	123.78	720	82.81
01/07/2024	21	21.9	720	96.96
01/08/2024	19	29.94	720	95.84
01/09/2024	11	18.05	720	97.49

El estudio de la implementación de redes privadas virtuales (VPN) para la interconexión de campus en la Universidad Estatal Amazónica (UEA) se centra en cómo estas soluciones han mejorado la seguridad, la disponibilidad y la resiliencia de los servicios de TI. A continuación, analizamos los resultados gráficos y su impacto en las variables clave:

Disponibilidad de los Enlaces de Internet (% de tiempo en línea)

$$Disponibilidad = \left(\frac{Tiempo\ operativo\ total - Tiempo\ de\ inactividad}{Tiempo\ operativo\ total}\right) x100$$

Figura 3 | Disponibilidad de los enlaces de Internet por Mes



El gráfico de disponibilidad de los enlaces de internet muestra una tendencia general positiva en la mayoría de los meses. Sin embargo, ciertas fluctuaciones destacan problemas en algunas sedes.

Análisis

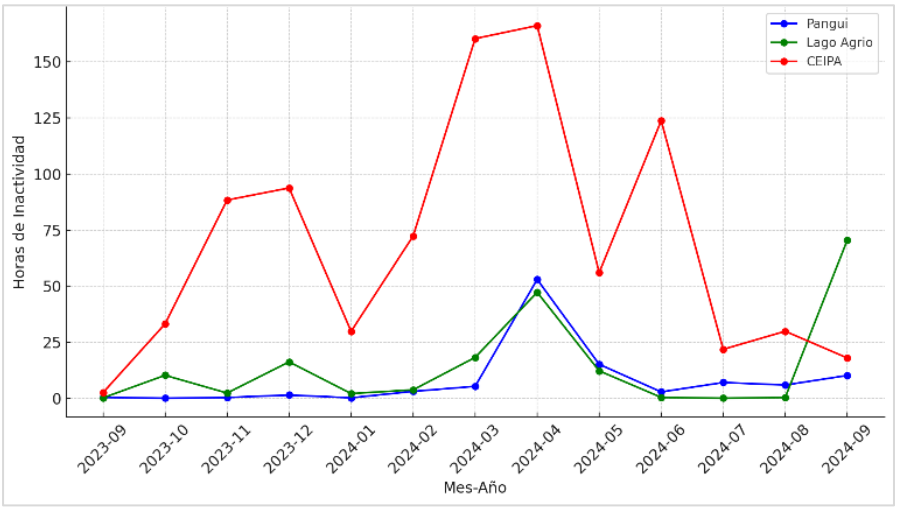
- Pangui y Lago Agrio presentan niveles de disponibilidad relativamente estables, con algunos meses alcanzando casi el 100%, lo que indica que la implementación de VPN y enlaces redundantes ha sido eficaz para garantizar la continuidad del servicio.
- CEIPA, por otro lado, muestra caídas significativas en algunos meses, lo que refleja problemas locales, posiblemente relacionados con el proveedor de suministro eléctrico, internet o la infraestructura interna de la sede.

Impacto

- Estos resultados demuestran que las decisiones estratégicas de implementar enlaces redundantes han reducido las interrupciones, mejorando la disponibilidad en general. Sin embargo, se debe prestar atención a la sede de CEIPA, que ha sido más vulnerable.
- La alta disponibilidad de los enlaces asegura que los servicios académicos y administrativos no se vean interrumpidos, lo que es esencial para el funcionamiento diario de la universidad.

Tiempo de Inactividad de los Servicios Críticos (Horas por Mes)

Figura 4 | Tiempo de inactividad de los servicios críticos (Horas por Mes)



El gráfico del tiempo de inactividad muestra un análisis del impacto directo de los fallos en la infraestructura de red sobre los servicios críticos en horas.

Análisis

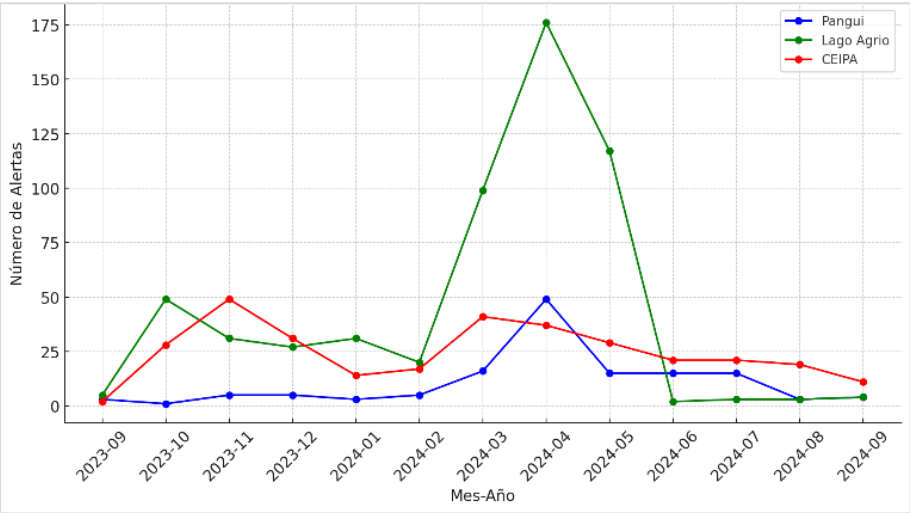
- Pangui y Lago Agrio mantienen tiempos de inactividad bajos y relativamente constantes, lo que indica un buen manejo de los problemas y fallos de red, posiblemente gracias al uso de tecnologías de alta disponibilidad.
- CEIPA, por otro lado, presenta picos elevados de tiempo de inactividad en ciertos meses, lo que sugiere una mayor frecuencia de problemas técnicos o fallos de infraestructura.

Impacto

- La baja cantidad de horas de inactividad en Pangui y Lago Agrio respalda la implementación de VPNs y enlaces redundantes como una solución exitosa para asegurar la continuidad de los servicios críticos.
- Los picos en CEIPA indican que, si bien la implementación ha sido efectiva en general, es crucial continuar mejorando la infraestructura en esta sede para alinearla con los estándares del resto de la universidad.

Números de Alertas generadas por Zabbix

Figura 5 | Número de alertas generadas por Zabbix por Mes



El gráfico del número de alertas de Zabbix muestra la cantidad de incidentes registrados por mes, lo que refleja la cantidad de fallos en los servicios de red monitoreados.

Análisis

- Pangui y Lago Agrio muestran una cantidad moderada de alertas, pero los números se mantienen relativamente controlados, lo que refleja una infraestructura de red bien gestionada.
- CEIPA muestra nuevamente un comportamiento más irregular con picos altos de alertas en algunos meses, lo que apunta a una mayor inestabilidad en esta sede en comparación con las otras.

Impacto

- Las alertas monitoreadas por Zabbix proporcionan información clave para el monitoreo continuo de la infraestructura de red. Los resultados sugieren que las mejoras en el sistema de monitoreo han permitido una gestión más eficiente de los incidentes en Pangui y Lago Agrio, reduciendo así el tiempo de inactividad.
- En CEIPA, la gran cantidad de alertas en ciertos meses indica que es necesario un análisis más profundo de la infraestructura para identificar y corregir las causas de los fallos frecuentes.

DISCUSIÓN

Los resultados obtenidos en la implementación de Redes Privadas Virtuales (VPN) y tecnologías de alta disponibilidad en la Universidad Estatal Amazónica (UEA) evidencian mejoras significativas en la interconexión de las sedes y en la seguridad y disponibilidad de los servicios de TI. Sin embargo, el

análisis detallado de los datos revela que aún persisten desafíos que deben ser abordados para alcanzar una interconexión totalmente efectiva y resiliente.

En primer lugar, la disponibilidad de los enlaces de internet muestra variaciones entre las diferentes sedes. Mientras que El Pangui y Lago Agrio presentan niveles de disponibilidad superiores al 99% en la mayoría de los meses, la sede de CEIPA experimenta fluctuaciones notables, con periodos donde la disponibilidad desciende hasta el 76.92%. Este comportamiento sugiere que, aunque la implementación de VPN y enlaces redundantes ha sido efectiva en general, existen factores adicionales que afectan la operatividad en ciertas sedes.

La alta frecuencia de caídas y tiempos de inactividad en CEIPA indica que, además de las soluciones tecnológicas implementadas, la estabilidad del suministro eléctrico y la infraestructura local desempeñan un papel crucial en la continuidad de los servicios. Las interrupciones en el suministro eléctrico pueden ocasionar caídas en los sistemas de red y afectar negativamente la disponibilidad de los servicios críticos. Por lo tanto, es evidente que la infraestructura energética es un componente esencial que debe ser considerado en el diseño y mantenimiento de la red institucional.

Además, el número de alertas generadas por Zabbix en CEIPA es significativamente mayor en comparación con las otras sedes, lo que refuerza la necesidad de fortalecer el monitoreo y el mantenimiento preventivo en esta ubicación. La alta incidencia de alertas podría estar relacionada con problemas recurrentes en la infraestructura de red o con la falta de redundancia en componentes críticos.

Otro aspecto relevante es que, si bien la implementación de VPN ha mejorado la seguridad y ha permitido una gestión centralizada, la interconexión no ha alcanzado aún su máximo potencial. La variabilidad en el desempeño entre sedes indica que la efectividad de la interconexión depende de un conjunto de factores más amplio que incluye no solo las tecnologías de red utilizadas sino también la infraestructura física, el mantenimiento continuo y la gestión de riesgos asociados a factores externos.

La presencia de riesgos como la inestabilidad del suministro eléctrico y la necesidad de energía redundante sugiere que, para garantizar un ecosistema de red robusto y confiable, es necesario adoptar un enfoque integral que incluya soluciones como sistemas de alimentación ininterrumpida (UPS), generadores de respaldo o incluso fuentes de energía alternativas como paneles solares.

Estas medidas contribuirían a minimizar el impacto de las interrupciones eléctricas y mejorarían la disponibilidad general de los servicios de TI.

Asimismo, el análisis de los resultados sugiere que es fundamental fortalecer las prácticas de mantenimiento y seguimiento en todas las sedes. La implementación de protocolos de mantenimiento preventivo más rigurosos, junto con un monitoreo continuo y detallado, permitiría identificar y solucionar problemas antes de que afecten significativamente la operatividad de la red.

Es importante destacar que la interconexión eficiente de las sedes ha permitido acortar distancias operativas, facilitando el soporte técnico y la provisión de servicios locales de manera más eficiente. Sin embargo, para maximizar estos beneficios, es necesario asegurar que todas las sedes cuenten con infraestructuras y prácticas de gestión alineadas y coherentes.

La implementación de tecnologías de alta disponibilidad y VPNs ha demostrado ser efectiva en mejorar la seguridad y disponibilidad de la red institucional, pero los resultados indican que, para alcanzar un nivel óptimo de operatividad, es imprescindible abordar también los factores externos y organizativos que influyen en el desempeño de la infraestructura de TI.

En este contexto, la experiencia de la UEA pone de manifiesto que la eficacia de las soluciones tecnológicas está intrínsecamente ligada a la calidad y estabilidad de la infraestructura física subyacente. La adopción de medidas complementarias que fortalezcan todos los componentes del ecosistema de red es esencial para consolidar los avances logrados y garantizar una interconexión plenamente efectiva entre todas las sedes.

CONCLUSIONES

La implementación de Redes Privadas Virtuales (VPN) y enlaces redundantes ha resultado en una notable mejora en la disponibilidad de los enlaces de internet en las sedes de El Pangui y Lago Agrio, alcanzando niveles superiores al 99% en varios meses. Este hallazgo coincide con estudios previos de RedCLARA (2015), que destacan cómo las VPNs pueden aumentar la disponibilidad y confiabilidad de las redes institucionales. Sin embargo, la variabilidad observada en la sede de CEIPA subraya la necesidad de abordar factores externos que afectan la disponibilidad, como la estabilidad del suministro eléctrico.

Las VPNs han demostrado ser efectivas para garantizar la seguridad de la transmisión de datos entre las sedes de la UEA, alineándose con las conclusiones de investigaciones de ISACA (2013) sobre la importancia de las VPNs en la protección de infraestructuras críticas. La centralización de la gestión de TI y la encriptación de datos han reducido significativamente la vulnerabilidad ante ciberataques, fortaleciendo la confidencialidad e integridad de la información académica y administrativa

A pesar de los avances tecnológicos, la falta de energía redundante en algunas sedes, particularmente en CEIPA, ha limitado la efectividad de las soluciones implementadas

Estudios como los de IEEE (2018) resaltan la importancia de sistemas de alimentación ininterrumpida (UPS) y fuentes de energía alternativas para mantener la operatividad de las redes. Implementar estas soluciones es esencial para garantizar la estabilidad y continuidad de los servicios de TI en todas las sedes de la UEA.

Los altos niveles de alertas y tiempos de inactividad en CEIPA indican que el mantenimiento y monitoreo continuo son cruciales para el rendimiento óptimo de la infraestructura de TI. La literatura existente, como la de Gartner (2020), enfatiza que un mantenimiento proactivo y un monitoreo riguroso son fundamentales para anticipar y resolver problemas antes de que afecten los servicios críticos. Fortalecer estos procesos en la UEA mejorará la eficiencia operativa y la resiliencia de la red.

La interconexión eficiente mediante VPNs ha facilitado una colaboración más estrecha entre las sedes de la UEA, mejorando el acceso a recursos académicos y administrativos. Este resultado está en línea con estudios de RedCLARA (2015) que demuestran cómo las VPNs pueden promover la cohesión y colaboración en instituciones educativas distribuidas geográficamente. La experiencia de la UEA confirma que una infraestructura de red bien gestionada es un facilitador clave para la colaboración institucional efectiva.

Los resultados indican que, aunque las tecnologías implementadas son robustas, su efectividad está condicionada por otros factores como la infraestructura física y la gestión de recursos. Esto refleja las conclusiones de estudios de ISACA (2013), que señalan que la tecnología por sí sola no garantiza el éxito sin un soporte organizativo y operacional adecuado. La UEA debe adoptar un enfoque integral que incluya mejoras en infraestructura física y capacitación continua del personal para maximizar los beneficios de las tecnologías implementadas.

La migración a plataformas como PFSense ha demostrado la importancia de elegir soluciones tecnológicas adaptables y escalables que puedan evolucionar con las necesidades de la institución. Este enfoque está respaldado por investigaciones de Gartner (2020), que destacan la necesidad de infraestructuras flexibles para soportar el crecimiento y los cambios tecnológicos. La capacidad de la UEA para escalar su infraestructura de TI ha sido fundamental para sostener la expansión y mejorar la gestión centralizada de sus redes.

REFERENCIAS BIBLIOGRÁFICAS

Chinkes, E. (2015). *Las Tecnologías de la Información y la Comunicación Potenciando la Universidad del Siglo XXI. RedCLARA*.

ISACA, «*Gobierno en la NUBE*» ISACA, Estados Unidos, 2013.

Secretaría de la Administración Pública. (2013). Decreto 166 - *Seguridad de la Información*. Quito.

International Organization for Standardization. (2013). ISO/IEC 27001:2013 - *Information technology — Security techniques — Information security management systems — Requirements*.

International Organization for Standardization. (2008). ISO/IEC 38500:2008 - *Information technology — Governance of IT for the organization*

Asamblea Nacional del Ecuador. (2008). *Ley de Protección de Datos Personales de Ecuador*.

Gobierno del Ecuador. (2013). *Esquema Gubernamental de Seguridad de la Información*.