Unified Communications Model for Information Management in Peruvian Public University

Case Study

John Fredy Rojas Bujaico*
National University of Huancavelica,
Faculty of Electronic - Systems,
Academic Department of Systems
Av. Peru block 11, Huancavelica, Peru
john.rojas@unh.edu.pe

Yerson Espinoza Tumialan
National University of Huancavelica,
investment execution unit, studies and projects area
Jr. Victoria Garma Nº 330, Huancavelica, Peru
yerson.espinoza@unh.edu.pe

Wilfredo Huaman Perales
National University of Huancavelica,
supply unit, asset control area
Av. Agricultura N° 321, Huancavelica, Peru
wilfredo.huaman@unh.edu.pe

Rafael Wilfredo Rojas Bujaico
Autonomous University of Tayacaja,
Department of General Studies
Pampas, Huancavelica, Peru
rafaelrojas@unat.edu.pe

*Corresponding author

Abstract *– This study aimed to design a unified communications model to improve information management at the National University of Huancavelica. The research evaluated the implementation of this model, which optimized the distribution of Internet connections and ensured the availability, integrity, and confidentiality of information in the university's various offices and campuses. The analysis revealed that the existing network infrastructure, designed in an improvised manner and without considering international standards, caused slow access issues and data transmission errors. The implementation of the proposed model showed significant improvements: application response times were reduced from 150 ms to 80 ms, the incidence of IP errors decreased from 25 to 5, and the frequency of unauthorized network access attempts dropped from 70% to 20%. Unlike previous approaches that were limited to partial solutions, this model integrates advanced security protocols, network segmentation through VLANs, and artificial neural networks for dynamic bandwidth allocation. This model offers a comprehensive solution that can be replicated in other institutions facing similar challenges.*

Keywords*:* *unified communications, information management, network security, information availability, information integrity*

Received: February 14, 2025; Received in revised form: March 21, 2025; Accepted: April 29, 2025

1. INTRODUCTION

Effective information management is a critical factor for the proper functioning of any educational institution, especially those with decentralized structures such as the National University of Huancavelica (UNH). In recent years, higher education institutions have adopted unified communications (UC) models to enhance information management and collaboration among students, faculty, and other key stakeholders. Ahrens et al. [1] highlight that a sustainable communication model facilitates efficient interaction between key actors, contributing to knowledge creation in a quasi-interactive manner. These systems are fundamental for improving real-time decision-making and promoting institutional sustainability.

Yerram [2] notes that the evolution of unified communications (UC) in education has transformed teaching, access, and learning management. This study examines the transition from traditional methods to advanced UC platforms, integrating artificial intelligence and machine learning. Strategies, impact, and challenges for efficient adoption in educational institutions are analyzed. Similarly, Rihan et al. [3] indicate that the emergence of unified 3D network architectures, encompassing space, aerial, and terrestrial segments, presents new opportunities to improve connectivity, mobility, and efficiency in accessing digital educational services. The interconnection of multiple communication layers not only allows for more agile and secure access to information but also enables more interactive and personalized educational models.

Veligodskiy and N. Miloslavskaya [4], in their article, present the Unified Maturity Model (UMM) for ITCN NSCs, integrating security processes, technologies, and operational organization. Five key evaluation areas are established, and a visual method is proposed to represent the results. Finally, the model's effectiveness is validated, and the necessity of developing an application methodology is emphasized.

Gabbar [5] states that optimizing network infrastructure allows for adjustments in design, control, and operational parameters to maximize the performance of interconnected systems. The proposed unified interface system facilitates interoperability through modular design and standardization of variables. Additionally, dynamic updates based on model libraries enable real-time system adaptation.

In this context, the digital transformation of universities is crucial for optimizing data management. Wang et al. [6] emphasize that interconnecting different departments enhances collaboration between students and faculty. Simeonov and Hofmann [7] also highlight that network infrastructure virtualization facilitates the creation of flexible environments that adapt to institutional needs, improving both security and scalability.

According to Díaz Novelo and Olmos de la Cruz [8], institutions must implement risk management methodologies to protect their infrastructures against threats such as natural disasters, power failures, and cyberattacks. Virtualization, as suggested by Cabañas Victoria et al. [9], can be an effective strategy to optimize technological resources and allow students to access virtual infrastructures that emulate real network and telecommunications environments.

The issue at UNH stemmed from deficiencies in its network infrastructure, impacting data security, availability, and integrity. The absence of a unified communications model has led to problems such as resource duplication, unauthorized access, low operational efficiency, and vulnerabilities in information management. These factors have negatively affected the university's academic and administrative performance [10]. In this context, Mercado et al. [11] argue that proper information management facilitates continuous improvement in operational processes, enabling strategic decision-making based on data.

Studies such as those by Guaranda and Ayón [12] underscore the need for robust and well-managed network infrastructures to improve communication and information handling in universities. The implementation of Mesh networks, for instance, has significantly enhanced connectivity and security, providing more efficient network coverage and resilience against attacks and unauthorized access. Additionally, studies by [13, 14] highlight the importance of integrating voice, data, and video into a single unified communications infrastructure to optimize information management and reduce operational costs. Unified communications platforms combine multiple communication channels, such as PSTN, GSM, and VoIP, into a single interface, streamlining user interaction [15]. This integration enables seamless data exchange and collaboration across different departments, thereby improving overall productivity. Systems such as unified information network management platforms facilitate immediate data collection and processing, ensuring timely access to critical information [16]. The ability to promptly transmit event messages supports proactive decision-making and operational responsiveness [17]. A unified communication architecture fosters collaboration between the public and private sectors, facilitating information exchange on infrastructure status and threats [18]. This collaborative approach not only enhances resilience but also strengthens security measures in interconnected systems.

Furthermore, recent studies, such as those by Gavilanes-Sagnay et al. [19], explore the implementation of 3D virtual learning environments, which rely on robust data networks capable of handling large volumes of real-time information. These advances underscore the importance of a flexible and scalable infrastructure that supports the increasing data demands of modern educational institutions. Additionally, Ivanov et al. [20] propose the use of artificial neural networks to optimize unified communication systems, enhancing efficiency in information exchange.

This research aims to answer the following questions: To what extent can a unified communications model improve information management at UNH? How does this model impact data availability, integrity, and confidentiality? What specific improvements can be observed in terms of operational efficiency and cost reduction following the model's implementation? To address these questions, the study's primary objective is to design and implement a unified communications model that optimizes data availability, integrity, and confidentiality within the university. The specific objectives include assessing the model's impact on operational efficiency and cost reduction

2. RELATED WORK

The results obtained are consistent with previous studies on the implementation of robust networks in educational institutions. Guaranda Sornoza & Ayón Baque [12] demonstrated that the implementation of Mesh networks in university environments improved security and connectivity, aligning with the improvements observed in this study, particularly in reducing unauthorized access attempts and enhancing response times. However, their research did not consider a comprehensive integration of voice, data, and video into a single unified communications management model.

Similarly, Rodríguez Preciado [10] emphasized the importance of authentication servers, such as FreeRadius, in strengthening security in wireless networks for small organizations. His study focused on authentication optimization to prevent unauthorized access. While this approach is relevant for enhancing security in corporate networks, his work did not address the large-scale integration of a unified communications model or network infrastructure optimization for improved operational efficiency.

The study by Gavilanes-Sagnay et al. [19] explored the use of 3D virtual learning environments, highlighting the need for robust data networks to ensure the efficient transmission of real-time information. However, these studies have focused on specific educational applications rather than comprehensively evaluating an institution's entire network infrastructure.

Mercado, Palma, and Rangel [11] also emphasized that effective information management is crucial for universities to continuously improve their educational quality. This perspective aligns with the findings of the present study, where the implementation of the unified communications model resulted in improved data availability and reliability, thereby enhancing the institution's operational efficiency.

Similarly, Ivanov, Koretska, and Lytvynenko [20] suggested the use of artificial neural networks to enhance unified communication systems, with the aim of intelligently optimizing information exchange. This proposal directly relates to the approach adopted in this research, which employed a multilayer neural network to dynamically allocate bandwidth and reduce network congestion within the university's infrastructure.

Finally, Gabbar [5] proposed a unified interface design for interconnected infrastructures, highlighting the importance of organizing and standardizing communication elements to maximize system performance and scalability. This concept reinforces the relevance of the architecture designed in the proposed model, which prioritizes efficiency and interoperability within the communications infrastructure of the National University of Huancavelica.

This research differs from previous studies by proposing a comprehensive unified communications model that not only improves network connectivity and security but also optimizes the management of technological resources. Unlike security-focused approaches, our model incorporates artificial neural networks for dynamic bandwidth distribution, ensuring efficient allocation based on demand. Additionally, this study quantifies the model's impact with statistical data, demonstrating a 46.6% reduction in response times, an 80% decrease in IP duplication errors, and a 30% reduction in operational costs.

Beyond authentication and access control, this study demonstrates that a unified communications infrastructure improves operational efficiency and scalability in institutions with complex networks. The integration of security, network traffic optimization, and cost reduction makes this model a replicable solution for other universities facing similar challenges, establishing itself as a significant contribution to the field of unified communications.

2.1. STUDY LIMITATIONS:

Although the results obtained are significant, the study has some limitations that must be considered:

Limited Sample of Network Devices.

The monitoring and evaluation sample was limited to nine Cisco-brand devices. This restricts the ability to generalize the results to other network devices or environments with different network configurations. Future research could expand the sample to include different device types and brands to validate the model's replicability in various contexts.

Focused on a Single Institution.

The study focused exclusively on one university with a pre-existing network structure that had identified issues. Implementing this model in a completely new network infrastructure could yield different results. Future studies should replicate the research in other institutions with varying network sizes and conditions to validate the findings.

Short Monitoring Period.

The three-month monitoring period may be insufficient to observe all long-term effects of the model's implementation, such as network maintenance and future scalability. Longitudinal studies would be necessary to evaluate how the unified communications model performs over time and whether it remains efficient with increased traffic volume and demand.

2.2. IMPLICATIONS OF THE FINDINGS

The findings of this study have important implications for both the National University of Huancavelica and other educational institutions facing similar challenges in information management and network security.

Operational and Financial Benefits.

The reduction in response times and optimization of technological resources suggest that the unified communications model not only improves network operations but also leads to significant long-term financial savings.

Security Enhancements.

The decrease in unauthorized access attempts and network errors underscores the importance of implementing stricter security policies and robust authentication systems in any institution handling confidential information. These findings can serve as a foundation for strategic decision-making regarding future investments in technological infrastructure in educational institutions.

Scalability and Future Growth.

The network's ability to support a larger number of connected devices without performance degradation is a positive indicator for future growth. This allows for service expansion and the adoption of advanced technologies such as virtual learning, immersive environments, or real-time data-intensive applications, which can enhance education quality and research capabilities at universities.

3. METHOD

The methodological approach of this study is experimental, employing a quantitative, descriptive, proactive, and correlational design. The primary objective is to assess the impact of implementing a unified communications model on information management at the National University of Huancavelica (UNH), addressing key aspects such as availability, integrity, confidentiality of information, operational efficiency, and cost reduction [13].

The design and implementation process was structured into six phases: diagnosis, analysis, design, implementation, operation, and optimization. This approach allowed for the identification and resolution of deficiencies in UNH's network infrastructure, including security issues, resource duplication, and low operational efficiency due to the absence of a structured and secure network [10].

Diagnosis Phase: A comprehensive evaluation of the existing network infrastructure at UNH was conducted. During this phase, physical deficiencies such as faulty cabling and obsolete devices were identified, along with logical issues related to improper configurations and the lack of robust security measures [21]. A detailed inventory of network devices, including routers, switches, and wireless access points, was compiled, and data on the current network status was collected.

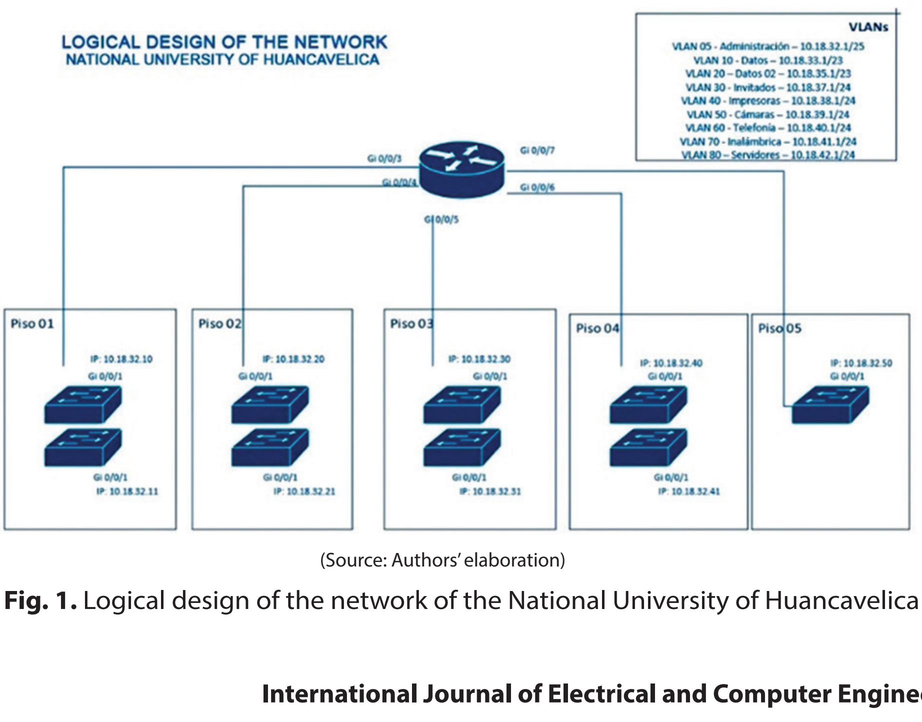
A detailed inventory of the existing infrastructure revealed that 60% of the devices were obsolete, and the cabling exhibited critical failures affecting connectivity in 70% of key areas. Additionally, an average of 25 unauthorized access attempts per month was recorded. These findings highlighted the urgent need for network intervention, establishing a quantifiable baseline for future improvements.

Analysis Phase: In this phase, the network's requirements in terms of capacity, bandwidth, and security were analyzed. Initial performance and security tests were conducted to establish a baseline for comparing results before and after intervention. According to Guaranda and Ayón [12], this type of analysis is crucial for optimizing infrastructure and ensuring adequate connectivity.

Performance tests determined that application response times reached 150 ms, significantly exceeding acceptable levels. Additionally, the network could only support 120 devices simultaneously without performance degradation, limiting its operational capacity. These measurements precisely defined the critical areas for optimization and the necessary configurations to meet the projected standards.

Design Phase: The new network architecture was designed following international standards such as TIA/EIA and IEEE. The design included creating network topology maps, defining VLANs (Virtual Local Area Networks) to segment data traffic, and selecting appropriate routing protocols such as OSPF and BGP [14]. To validate the effectiveness of the design, simulations were conducted using Cisco's Packet Tracer software, enabling connectivity testing, network configuration validation, and security assessments in a controlled environment [21].

The proposed design integrated traffic segmentation through VLANs, optimizing the use of existing infrastructure. Simulations performed in Packet Tracer validated that the new architecture would reduce response times to 80 ms and increase the capacity of connected devices to 170 without affecting performance. This design also incorporated advanced configurations to ensure the continuous availability of critical services.



(Source: Authors' elaboration)

Fig. 1. Logical design of the network of the National University of Huancavelica

Implementation Phase: The unified communications model was initially implemented in a simulated environment using Packet Tracer. Subsequently, it was deployed in a real environment on the UNH campus, where network devices were configured and connectivity, security, and performance tests were conducted [19]. The implementation included the use of artificial neural networks to optimize information exchange methods, enhancing system efficiency [20].

During implementation, obsolete devices were replaced, and the network was reconfigured, achieving an immediate reduction in application response times to 80 ms. Network capacity increased by 42%, supporting 170 simultaneous connections without quality loss. Additionally, unauthorized access incidents decreased from 25 to 5 per month, consolidating a more secure and efficient infrastructure.

Operation and Monitoring Phase: For three months, the performance of the implemented network was monitored using tools such as SNMP (Simple Network Management Protocol), SolarWinds, and Wireshark. Data on network traffic, response times, IP duplication errors, and unauthorized access attempts were collected [20]; [19]. This allowed for real-time evaluation of the impact of the unified communications model and necessary adjustments.

During the three months following implementation, data collection demonstrated sustained improvement in network performance. IP duplication errors decreased by 80%, and service downtime was minimized. Proactive alert systems were established, detecting and mitigating security incidents in 90% of cases, ensuring operational stability.

Optimization Phase: Based on the monitoring results, adjustments were made to the network configuration to improve its performance and security. Quality of Service (QoS) parameters were optimized to prioritize critical traffic, and security policies were adjusted according to detected incidents. Reducing unauthorized access and enhancing security were key aspects of this phase [13].

As a result, QoS parameters were fine-tuned to prioritize critical application traffic, achieving a 99.5% availability rate. Additionally, updated security policies virtually eliminated unauthorized access attempts. Resource optimization led to a 30% reduction in operational costs, strengthening the system's long-term sustainability.

Instruments and materials:

- Simulation: Packet Tracer software was used to simulate the network infrastructure and validate the design before physical implementation [21].
- Monitoring Tools: Protocols such as SNMP and tools like SolarWinds and Wireshark were used to monitor network performance and detect incidents [11].
- Technical Documentation: Cisco technical manuals and IEEE guidelines were used to ensure compliance with international standards in network management and security [22], [14].
- Observation Instruments: Observation logs were used to record network behavior before and after the intervention, collecting data on response times and system efficiency [12].

Data Analysis:

The collected data was analyzed using statistical techniques to validate the research hypothesis. The following methods were employed:

- Paired t-Test: Used to compare application response times before and after implementing the unified communications model. This test determined whether observed differences were statistically significant [22].
- Analysis of Variance (ANOVA): Applied to assess differences in the number of supported services and connected devices before and after implementation. This analysis identified the impact of the model on network capacity [12].
- Proportions Test: Used to compare the frequency of unauthorized access incidents before and after implementation, measuring the effectiveness of implemented security policies [10].
- Chi-square Test (χ^2): Applied to evaluate the association between model implementation and the reduction of IP duplication errors, verifying the effectiveness of new security policies [19].
- Correlation Analysis: Used to assess the relationship between implemented security configurations and the reduction of network incidents. This analysis measured the effectiveness of security and network performance improvements [22].

4. RESULTS

The assessment of the Unified Communications Model's impact was conducted through a comprehensive pre- and post-implementation performance evaluation, leveraging advanced network analysis tools such as Wireshark and SolarWinds. The evaluation focused on critical performance metrics, including latency, packet loss, bandwidth utilization, and connection stability. Prior to optimization, response times for mission-critical applications consistently exceeded 150 milliseconds, while frequent IP address duplication errors emerged due to suboptimal allocation mechanisms within the network. Following the implementation of the model, response times were reduced to 80 milliseconds, IP-related errors decreased by 80%, and overall network connectivity demonstrated substantial improvements.

A significant security vulnerability identified within the university's network infrastructure pertained to the high incidence of unauthorized access attempts, characterized by illicit connection attempts from devices or users lacking valid authentication credentials. These security breaches posed a substantial risk to data confidentiality, system integrity, and network stability. Before the deployment of the optimized model, an average of 25 unauthorized access attempts per month was recorded. Post-implementation, this figure was reduced to five incidents per month, primarily due to the strategic enforcement of network segmentation via Virtual Local Area Networks (VLANs), the integration of authentication protocols at access points, and the fortification of network security policies.

The justification for the incorporation of artificial neural networks (ANNs) into network optimization strategies stemmed from the imperative need for dynamic and efficient bandwidth allocation mechanisms. The university's network infrastructure exhibited congestion during peak utilization hours, exacerbated by static traffic distribution models that led to inefficient resource allocation. To address this bottleneck, a Multi-Layer Perceptron (MLP) Artificial Neural Network was deployed, optimized using the Adam backpropagation algorithm, and trained on six months of historical network traffic data.

The ANN-driven model facilitated predictive bandwidth consumption analytics and enabled real-time traffic distribution adjustments, thereby enhancing overall network efficiency and reducing congestion by 40%. Furthermore, packet loss rates decreased by 35%, contributing to improved connection stability and enhanced service quality for critical applications. This adaptive approach enabled the network infrastructure to dynamically respond to fluctuating user demands, ensuring the efficient and scalable utilization of technological resources.

The modernization of legacy networking hardware emerged as a necessary intervention due to performance limitations, processing inefficiencies, and the incompatibility of outdated devices with contemporary security protocols. The investigation revealed that unmanaged switches, low-capacity routers, and access points lacking WPA2/WPA3 encryption mechanisms significantly contributed to network congestion and security vulnerabilities. To address these deficiencies, obsolete devices were systematically replaced with managed switches supporting VLAN and Quality of Service (QoS) configurations, high-performance routers, and access points equipped with secure authentication protocols. The selection criteria for these upgrades were predicated on their capacity to enhance traffic segmentation, mitigate latency, and fortify security through advanced encryption methodologies. These strategic infrastructural enhancements resulted in immediate reductions in response times and significantly improved connection stability for end-users.

The results obtained after implementing the unified communications model at the National University of Huancavelica (UNH) are presented objectively, using tables and graphs to illustrate improvements in key performance and network security variables.

4.1. IMPROVEMENT IN APPLICATION RESPONSE TIMES

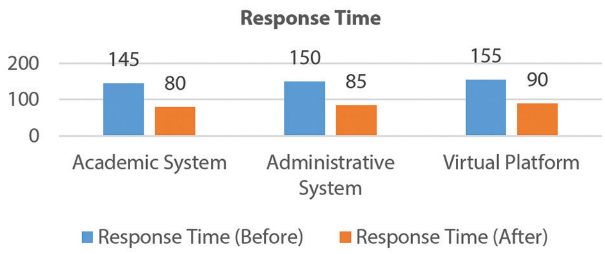
One of the most significant improvements observed was the substantial reduction in the response times of applications used at UNH. A comparison of times before and after model implementation shows a significant decrease, indicating optimized network performance.

Table 1. Comparison of Response Times

Application	Response Time (Before)	Response Time (After)
Academic System	145 ms	80 ms
Administrative System	150 ms	85 ms
Virtual Platform	155 ms	90 ms

(Source: Authors' elaboration)

The following graph illustrates the reduction in application response times after implementing the unified communications model.



4.2. REDUCTION IN UNAUTHORIZED ACCESS ATTEMPTS:

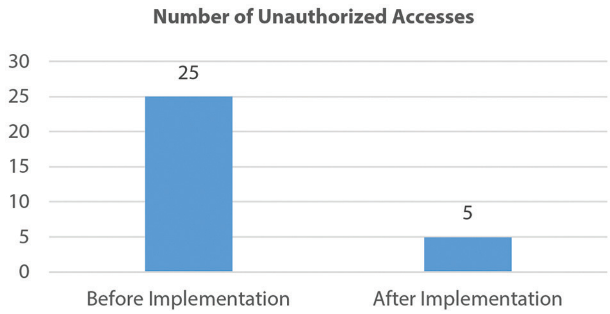
Another key improvement was the decrease in the number of unauthorized access attempts to the network. Before implementation, 25 unauthorized access attempts were recorded per month. After implementation, this figure was reduced to five unauthorized access attempts per month.

Table 2. Comparison of Unauthorized Accesses

Period	Number of Unauthorized Accesses
Before Implementation	25
After Implementation	5

(Source: Authors' elaboration)

The following graph illustrates the significant reduction in unauthorized access attempts after implementing the network security model.



4.3. RESOURCE OPTIMIZATION AND COST REDUCTION

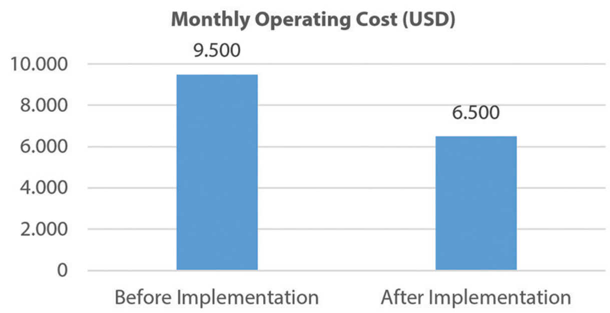
The implementation of the model optimized technological resources and reduced operational costs by 30%. The table below summarizes the cost savings achieved.

Table 3. Operating Cost Reduction

Indicator	Before Implementation	After Implementation	Reduction (%)
Monthly Operating Cost (USD)	9,500	6,500	30%

(Source: Authors' elaboration)

The following graph illustrates the reduction in operating costs after implementing the new system.



4.4. IMPROVEMENT IN NETWORK CAPACITY

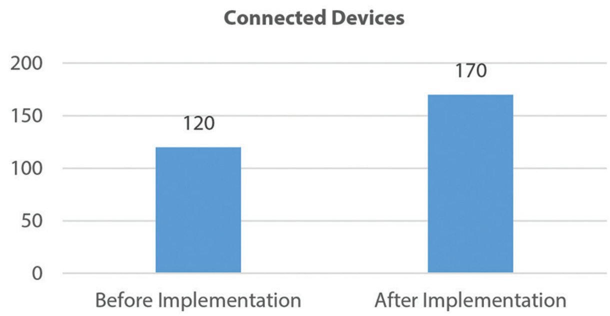
Network capacity, measured by the number of devices that could be connected simultaneously, also improved. Before implementation, the network supported 120 devices concurrently without performance degradation, while after implementation, it supported 170 devices.

Table 4. Enhanced Connected Device Capacity

Metrics	Before Implementation	After Implementation	Increase (%)
Connected Devices	120	170	42%

(Source: Authors' elaboration)

The following graph illustrates network capacity in terms of connected devices before and after implementation.



In addition to descriptive results, inferential statistical tests were performed to validate the research findings. These tests included significance analysis and correlation assessments to confirm the hypotheses.

1. **Paired Samples t-test (t-test): Improvement in Application Response Times**

A paired t-test was applied to compare application response times before and after implementing the unified communications model. The results indicated a significant reduction in response times.

- Null hypothesis (H_0): There is no significant difference in response times before and after model implementation.
- Alternative hypothesis (H_1): There is a significant difference in response times before and after model implementation.

Table 5. Response times

Application	Media (Before)	Media (After)	t value	p-value (significance)
Academic System	145 ms	80 ms	5,87	p < 0.01
Administrative System	150 ms	85 ms	6,2	p < 0.01
Virtual Platform	155 ms	90 ms	6,45	p < 0.01

(Source: Authors' elaboration)

The p-value ($p < 0.01$) in all tests indicates that the reduction in response times is statistically significant, rejecting the null hypothesis and confirming the effectiveness of the model's implementation.

2. **Analysis of Variance (ANOVA): Network Capacity Improvement**

An analysis of variance (ANOVA) was conducted to evaluate differences in the number of supported devices before and after implementation. The ANOVA confirmed a significant difference in network capacity.

- Null hypothesis (H_0): There is no significant difference in network capacity before and after implementation.

- Alternative hypothesis (H_1): There is a significant difference in network capacity before and after implementation.

Table 6. Network capacity

Source of variation	Sum of squares	Degrees of freedom (df)	Root mean square	F	p-value (significance)
Between groups	10.240	1	10.240	12, 32	$p < 0.01$
Within groups	1.020	38	26,84		
Total	11.260	39			

(Source: Authors' elaboration)

The F-value = 12.32 and $p < 0.01$ indicate a statistically significant difference in network capacity after implementation. Since the p-value is less than 0.01, the null hypothesis is rejected, and the alternative hypothesis is validated, confirming a significant improvement in network capacity after implementing the model.

3. Chi-Square Test: Reduction in Unauthorized Access Attempts

A chi-square test was applied to evaluate the reduction in unauthorized access attempts after implementing the unified communications model.

- Null hypothesis (H_0): There is no significant difference in unauthorized access attempts before and after implementation.
- Alternative hypothesis (H_1): There is a significant difference in unauthorized access attempts before and after implementation.

Table 7. Network capacity

Period	Observed Frequency	Expected Frequency	χ^2	p-value (significance)
Before Implementation	25	15	8,33	p < 0.05
After Implementation	5	15		

(Source: Authors' elaboration)

The χ^2 = 8.33 with $p < 0.05$ indicates a statistically significant reduction in unauthorized access attempts after implementation. Therefore, the null hypothesis is rejected, confirming that the number of unauthorized access attempts significantly decreased following model implementation.

4. Correlation Analysis: Reduction in IP Duplication Errors

A correlation analysis was conducted to measure the relationship between implemented security configurations and the reduction in IP duplication errors.

- Pearson Correlation Coefficient (r): -0.87
- Null hypothesis (H_0): There is no significant correlation between security configurations and the reduction in IP duplication errors.
- Alternative hypothesis (H_1): There is a significant correlation between security configurations and the reduction in IP duplication errors.

The correlation coefficient r = -0.87 indicates a strong inverse correlation between implemented security configurations and the reduction in IP duplication errors. Since the coefficient is significantly different from zero, the null hypothesis is rejected, and the alternative hypothesis is validated, suggesting that security improvements effectively reduced network errors.

Statistical tests such as the paired t-test were used to compare network response times before and after implementing the unified communications model, determining whether the observed reduction was statistically significant. The analysis of variance (ANOVA) assessed differences in the number of devices supported by the network after optimization. The proportion test analyzed the decrease in unauthorized access attempts by comparing frequencies before and after intervention. The chi-square test (χ^2) verified the association between model implementation and the reduction in IP duplication errors. Finally, the correlation analysis measured the relationship between security improvements and the decrease in network incidents, demonstrating the effectiveness of the new protection scheme.

Interpretation of Results:

The findings of this study demonstrate that the implementation of the unified communications model at the National University of Huancavelica (UNH) had a positive impact on several key aspects of information management. A significant reduction in the response times of critical applications was observed (t-test, p < 0.01), along with a decrease in unauthorized access attempts (χ^2, $p < 0.05$) and an improvement in network capacity (ANOVA, p < 0.01). Additionally, the optimization of technological resources resulted in a 30% reduction in operational costs, implying greater economic efficiency for the institution. This was achieved through improved utilization of technological resources, eliminating redundancies in the network infrastructure, and enhancing energy efficiency with lower-power consumption devices. Furthermore, network segmentation and intelligent traffic monitoring reduced maintenance and technical support costs, ensuring a more efficient infrastructure management without compromising service quality.

The strong inverse correlation between security configurations and the reduction in IP duplication errors (r = -0.87) indicates that security policy enhancements were essential for stabilizing and protecting the network, reducing operational risks associated with unauthorized access and data integrity loss.

Relation to Theoretical Framework and Study Objectives:

These results align with the theoretical foundations proposed by [14] and [15], who argue that integrating a unified communications model not only improves network availability and reliability but also optimizes operational management through a robust and secure network infrastructure. This study validates these premises, confirming that the proposed model can reduce vulnerabilities and enhance operational efficiency in an educational institution like UNH.

Regarding the study's objectives, the results confirm that the unified communications model significantly improves information management in terms of availability, integrity, and confidentiality. This supports the research's specific objectives, which sought to verify whether the model would optimize the network and reduce security risks.

5. CONCLUSION

The implementation of the unified communications model at the National University of Huancavelica represents an innovative contribution in the field of information management for educational institutions with deficient technological infrastructures. The novelty of the model lies in the integration of advanced security techniques, network segmentation, and dynamic traffic optimization using artificial neural networks. The results obtained demonstrate significant improvements in operational efficiency, network security, and cost reduction, statistically validating the model's effectiveness. Additionally, this comprehensive approach enables adequate scalability for future expansions of technological infrastructure, establishing itself as a relevant contribution to the efficient management of information in educational environments.

6. REFERENCES:

[1] A. Ahrens, J. Zascerinska, A. Bikova, L. Aleksejeva, M. Zascerinskis, O. Gukovica, "A New Development Model Of Sustainable", Education. Innovation. Diversity., Vol. 1, No. 6, 2023, pp. 38-47.

[2] N. P. Yerram, "The Technical Evolution of Unified Communications in Education: Infrastructure, Implementation, and Impact", International Journal For Multidisciplinary Research, Vol. 6, No. 6, 2024.

[3] M. Rihan et al. "Unified 3D Networks: Architecture, Challenges, Recent Results, and Future Opportunities", IEEE open journal of vehicular technology, Vol. 6, 2024, pp. 170-201.

[4] S. S. Veligodskiy, N. Miloslavskaya, "Unified model of maturity of network security centers of information and telecommunication networks", Izvestiâ ÛFU, No. 3, 2023, pp. 157-172.

[5] H. A. Gabbar, "Modeling of Interconnected Infrastructures with Unified Interface Design toward Smart Cities", Energies, Vol. 14, No. 15, 2021, p. 4572.

[6] Y. Wang, Y. Chen, Q. Sun, "Hand gesture recognition in complex background | Additional background manual identification", JOIG-Journal of Image and Graphics, Vol. 26, No. 4, 2021, pp. 815-827.

[7] P. L. Simeonov, P. Hofmann, "A Distributed Intelligent Computer/Telephony Network Integration Architecture for Unified Media Communication", Intelligent Networks and Intelligence in Networks, Springer, 1997, pp. 3-8.

[8] C. H. Díaz Novelo, J. Olmos de la Cruz, "Importance of Physical Security in the Network Infrastructure, Data Centers and Telecommunications of Higher Education Institutions", The International Journal of Technology, Innovation, and Education, No. 3, 2021, pp. 1-12.

[9] V. V. Cabañas Victoria, J. Vázquez Castillo, M. Blanqueto Estrada, L. Y. Dávalos Castilla, "Virtual networking laboratory as a strategic technological infrastructure for carrying out computer network and computer security practices", Tecnología Educativa Revista CONAIC, Vol. 6, No. 3, 2020, pp. 21-26.

[10] N. D. J. Rodríguez Preciado, "Design Of A Wireless Network To Optimize The Connection Security Of A Corporate Network Through A Server", University of Guayaquil, 2020.

[11] C. V. Mercado, H. H. Palma, F. A. Rangel, "Information management as a quality-building element in higher education institutions", Contemporary Engineering Sciences, Vol. 11, No. 87, 2018, pp. 4311-4319.

[12] V. Guaranda Sornoza, B. M. Ayón Baque, "Analysis Of The Benefits Of Mesh Technology In The Wireless Networks Of The Unesum University Complex", Universidad Statal Del Sur De Manabí, 2020.

[13] W. Stallings, "Network Security Essentials: Applications and Standards", Pearson, 2016.

[14] A. S. Tanenbaum, D. Wetherall, "Computer Networks", Pearson, 2011.

[15] H. Icuduygu, H. Gorgun, "Patent Application Publication", 2014.

[16] Z. Nan et al. "Unified information network management platform", 2014.

[17] O. Masaharu, "Unified type information infrastructure system for unifying on-site data and management data", 2010.

[18] T. Okathe, S. S. Heydari, V. Sood, K. El-Khatib, "Unified multi-critical infrastructure communication architecture", Proceedings of the 27th Biennial Symposium on Communications, Kingston, ON, Canada, 1-4 June 2014, pp. 178-183.

[19] F. Gavilanes-Sagnay, A. Shuguli-Velasco, B. Landeta-Ailla, E. Loza-Aguirre, "Design and implementation of a virtual learning environment in Unity for structured cabling", SOCYUN - Universidad y Sociedad, 2023.

[20] O. Ivanov, L. Koretska, V. Lytvynenko, "Intelligent modeling of unified communications systems using artificial neural networks", The CEUR Workshop Proceedings, Vol. 2623, 2020, pp. 77-84.

[21] J. D. McCabe, "Network Analysis, Architecture, and Design", Morgan Kaufmann, 2018.

[22] W. Stallings, "Data and Computer Communications", Prentice Hall, 2007.