DEPÓSITO LEGAL ZU2020000153
ISSN 0041-8811
E-ISSN 2665-0428

# Revista de la Universidad del Zulia

Fundada en 1947
por el Dr. Jesús Enrique Lossada

## Ciencias del Agro Ingeniería y Tecnología

Año 12 N° 32
Enero - Abril 2021
Tercera Época
Maracaibo-Venezuela

**DOI:** http://dx.doi.org/10.46925//rdluz.32.21

# Modelo de seguridad informática para un medio de conexión pública

Gilberto Carrión-Barco*
Manuel-Jesús Sánchez-Chero **
Consuelo Ivonne Del Castillo Castro***
Freddy William Campos Flores****
Marcos Timaná Alvarez *****

RESUMEN

Hoy en día, las organizaciones hacen todo lo posible para mantener el control y ayudar a proteger sus redes corporativas y su activo de información de las amenazas cibernéticas, es por ello que se hace necesario garantizar la seguridad de los datos mientras viaja por la red pública. Frente a esta situación se circunscribe la presente investigación, teniendo como propósito la elaboración de un modelo de seguridad informática que garantice el intercambio de información académica para un medio de conexión pública entre la Universidad Nacional Pedro Ruiz Gallo y el Centro Pre Universitario de la entidad. El estudio fue de tipo aplicada, con un alcance cuantitativo – explicativo y diseño no experimental de tipo trasversal. La muestra estuvo constituida por un total de 29 técnicos especialistas en tecnologías de la información de las diferentes oficinas de la Universidad, el instrumento utilizado fue el cuestionario, el cual estuvo conformado por 20 reactivos divido en dos dimensiones: conexión de la red y seguridad informática. Como resultado se logró determinar que la conexión de la red y la seguridad informática se encuentran en un nivel bajo y deficiente, respectivamente, por lo que se concluye que la elaboración de un modelo de seguridad informática para VPN permitirá intercambiar información académica de manera segura ente los dos sitios.

PALABRAS CLAVE: Modelo, intercambio, información, seguridad informática, VPN.

*Docente Auxiliar. Universidad Nacional Pedro Ruiz Gallo. Perú. ORCID: https://orcid.org/0000-0002-1104-6229.

**Docente Investigador. Universidad Nacional de Frontera. Perú. ORCID: https://orcid.org/0000-0003-1646-3037. E-mail: manuelsanchezchero@gmail.com

*** Docente Asociado. Universidad Nacional Pedro Ruiz Gallo. Perú. ORCID: https://orcid.org/0000-0002-1512-006X.

**** Docente Asociado. Universidad Nacional Pedro Ruiz Gallo. Perú. ORCID: https://orcid.org/0000-0002-9624-2930.

***** Docente Auxiliar. Universidad Nacional de Frontera. Perú. ORCID: https://orcid.org/0000-0002-4222-7372

Recibido: 25/09/2020 Aceptado: 19/11/2020

DOI: http://dx.doi.org/10.46925//rdluz.32.21

# Computer security model for a public connection medium

ABSTRACT

Today, organizations do everything possible to maintain control and help protect their corporate networks and their information assets from cyber threats, which is why it is necessary to guarantee data security while traveling through the public network , Faced with this situation, this research is circumscribed, having as its purpose the elaboration of a computer security model that guarantees the exchange of academic information on a means of public connection between the Pedro Ruiz Gallo National University and the Pre-University Center of the entity . The study was of an applied type, with a quantitative-explanatory scope and a non-experimental cross-sectional design. The sample consisted of a total of 29 specialists in information technology from the different offices of the University, the instrument used was the questionnaire, which was made up of 20 items divided into two dimensions: network connection and computer security. As a result, it was possible to determine that the network connection and computer security are at a low and deficient level respectively, so it is concluded that the development of a computer security model for VPN will allow the exchange of academic information in a secure way between the two sites.

KEYWORDS: Model, exchange, information, computer security, VPN.

## Introducción

Actualmente los sistemas de información, los datos contenidos en ellas y la información son los activos más valiosos para las organizaciones, por lo que se hace necesario brindarles una protección adecuada frente a las posibles intrusiones derivadas de las vulnerabilidades existentes en sus sistemas de seguridad (Solarte et al., 2015).

En cuanto al estado actual de la seguridad informática en Latinoamérica, según Deloitte (2016), las tendencias en cuanto a la gestión de ciber-riesgos y seguridad informática indican que el 20% de las empresas no tienen centralizado en un área las operaciones de seguridad, por lo que 4 de cada 10 de estas organizaciones fueron vulneradas en la seguridad de sus datos en los últimos 2 años.

Por su parte, las Redes Privadas Virtuales (VPN) de acceso remoto posibilitan a los usuarios implantar una conexión segura a una red informática en una ubicación remota; por lo que es indispensable proteger la VPN para evitar la pérdida de datos del usuario. Deshmukh & Iyer (2017) menciona que el concepto de "*Office from home*" se viene desarrollando ampliamente.

DOI: http://dx.doi.org/10.46925//rdluz.32.21

Las organizaciones transnacionales también están promoviendo este concepto porque es beneficioso para aumentar las horas de trabajo y su eficiencia. En ese sentido, Deshmukh & Iyer (2017) realizaron una encuesta donde mencionan que para el 2025, casi el 50% de las organizaciones adoptarán el concepto anterior. En este caso, los usuarios necesitan acceso remoto a los servidores de la oficina y de la organización.

Como menciona Aung & Thein (2020), en la actualidad las VPN se han convertido en la tecnología más importante y vital para todos los usuarios que están interesados en preservar su privacidad. Mundialmente, Internet maneja alrededor de 71.131 GB de tráfico por segundo; 2.790.265 correos electrónicos y 73.849 búsquedas de Google por segundo. Según la encuesta desarrollada por Ponemon Institute (Ponemon Institute, 2018), el 67% de las pymes admitieron haber sido atacadas en 2018. Por lo tanto, las VPN, son una manera competente que puede resguardar toda la información a través del uso de Internet evitando que se utilice de manera equivocada.

La información es considerada como un activo muy importante para las organizaciones. Las universidades requieren de esta información para realizar sus operaciones cotidianas (Tang et al., 2016). Sin embargo, con el devenir de la tecnología emergen nuevas formas de ataque que ponen en riesgo la información académica. Internet al ser una red pública, constituye una gran puerta por la cual ingresan constantes ataques que logran vulnerar la seguridad informática de la organización (Sohrabi Safa et al., 2016).

En este sentido, las aplicaciones informáticas, las aplicaciones de red y las tecnologías de la información, cumplen un rol preponderante en el contexto de las universidades. Los campus universitarios están demostrando ser uno de los lugares con mayor tecnología desplegada en sus recintos al ofrecer servicios con soporte en Wi-Fi, aprendizaje remoto, servicios de biblioteca digitales, virtualización de cursos, entre otros. Todo este avance conlleva a que la infraestructura informática de la universidades sea vulnerable, que constantemente se someta a ataques y la información se vea expuesta a diferentes tipos de amenazas por parte de usuarios mal intencionados que tratan de vulneran los controles informáticos (Joshi & Singh, 2017).

Los centros superiores de estudio afrontan una problemática relacionada con las medidas de seguridad de la información, mientras que por un lado se denota un bajo compromiso en

DOI: http://dx.doi.org/10.46925//rdluz.32.21

mejorar la seguridad, por otra parte se dificulta implementar políticas y controles para garantizar la protección de los datos; existen razones para que se produzca lo antes mencionado: falta de capacitación al personal, inadecuada aplicación de políticas de seguridad, desconocimiento de vulnerabilidades y compromiso de la organización con la seguridad informática (Esparza et al., 2020).

En el ámbito local, la Universidad Nacional Pedro Ruiz Gallo (UNPRG) tiene dentro de su estructura orgánica a la Unidad de Infraestructura Tecnológica área que depende de la Oficina General de Sistemas Informáticos; esta oficina tiene como responsabilidad el diseño, planificación, actualización y supervisión de los sistemas informáticos administrativos, académicos y de investigación de la entidad (Estatuto UNPRG, 2017).

La UNPRG, localizada en la ciudad de Lambayeque, intercambia información académica con el Centro Pre Universitario (CPU), el cual se encuentra localizado en la ciudad de Chiclayo, ambos sitios se conectan por medio de la red pública internet. Conocedores de esta realidad problemática suscitada en muchas universidades y en particular en la UNPRG, se plantea la siguiente pregunta de investigación: ¿De qué manera se puede garantizar el intercambio de información académica sobre un medio de conexión pública entre la UNPRG con el CPU de la entidad?

Diversas investigaciones han contribuido con el problema en estudio, tal es el caso de Jing et al. (2016), quienes manifiestan que actualmente el uso de varios campus universitarios junto al intercambio de información son actividades muy comunes que han conllevado a una gran demanda de acceso remoto, lo cual requiere mayor cantidad de requisitos para que la arquitectura de red logre firmeza y eficacia. El objetivo de esta investigación consistió en diseñar una arquitectura de acceso VPN basada en red multi-ISP, combinada con tecnología IPSec VPN y L2TP, priorizando el esquema de referencia para conexiones de redes VPN empresariales. La exitosa implementación de la red planteada puede facilitar una referencia vigorosa de la red de varios campus de conexión para colegios, universidades y empresas.

Como expresan Wu & Xiao (2019), la seguridad de las comunicaciones en Internet se ha convertido en un tema fundamental. La VPN es un método de solución que viene siendo empleada por muchos años, encargada de establecer una red privada que hace uso de tecnología

DOI: http://dx.doi.org/10.46925//rdluz.32.21

de túneles en el público; de modo que el objetivo de este documento fue examinar el impacto del desempeño de VPN con diferentes topologías en el campus de red de la Universidad Normal de Beijing, haciendo uso de indicadores de prueba, remitente y receptor, finalmente de la arquitectura experimental. Llegando a la conclusión que al diseñar una topología VPN, se recomienda una topología estrella o en árbol, además del rendimiento de la VPN con el protocolo Softether, superior al del Protocolo L2TP.

Amankwa et al. (2014) mencionan que la seguridad informática alude a la información técnica, dificultades de seguridad e información no técnica (relacionada con las personas), pero la investigación se centra principalmente en problemas técnicos, por lo que se ignoran los problemas no técnicos en relación con las personas. En esa misma línea, Li yong (2015), refiere que la conectividad de la red es un parámetro de gran importancia para medir la confiabilidad de la configuración de la red. Generalmente se usa para analizar la vulnerabilidad, supervivencia y confiabilidad de las redes de comunicación.

A todo esto, tal como menciona Altamirano (2019), los sistemas de información (SI) que en las instituciones educacionales se manipulan, en ocasiones están encaminados hacia la misión de la organización, que por lo general poseen un entorno hostil; es por esto que la seguridad informática es una disciplina que integra un conjunto de políticas, procesos, procedimientos, estructuras organizacionales y funciones para ayudar a proteger la confidencialidad, integridad, disponibilidad de los recursos gestionados por los SI independientemente del formato que tengan, sean electrónicos o papel.

Finalmente, esta investigación se justifica puesto que, con la elaboración del modelo seguridad informática se garantizará el envío de información de manera segura sobre un medio de conexión pública poco confiable, como internet entre la UNPRG y el CPU; así mismo, se mejorará el intercambio de información académica contextualizada, permitiendo a su vez que el personal incremente su producción en beneficio de la comunidad universitaria. Así mismo, el presente estudio tiene como objetivo elaborar un modelo de seguridad informática que garantice el intercambio de información académica sobre un medio de conexión pública entre la UNPRG con el CPU de la entidad.

**DOI:** http://dx.doi.org/10.46925//rdluz.32.21

## 1. Metodología

La investigación es aplicada, teniendo un alcance cuantitativo – explicativo y diseño no experimental de tipo trasversal (Bernal, 2010). La muestra estuvo constituida por el conjunto de técnicos especialistas en tecnologías de la información de las diferentes facultades, así como de la oficina de asuntos académicos, de la oficina general de admisión y de la oficina general de sistemas informáticos de la UNPRG, contando con un total de 29 sujetos. Así mismo, como criterios de exclusión se tiene al personal técnico contratado especialista en tecnologías de la información de las diferentes facultades y oficinas de la UNPRG.

El instrumento estuvo conformado por 20 reactivos divido en dos dimensiones: la primera dimensión corresponde a la conexión de la red; la segunda dimensión se adentra en la seguridad informática. La información recolectada por medio de los instrumentos ha sido validada a través de métodos de consistencia interna (Hernández-Sampieri et al., 2018), teniendo una confiabilidad a través de estadístico de alfa de Cronbach de 0.817, quedando así revelado que la información obtenida fue apta para ser analizada. Posteriormente, con el libro electrónico Microsoft Excel y el software estadístico SPSSv4, se procedió a procesar los datos, en donde no solo se limitó a la recolección de datos sino a la predicción e identificación de las relaciones que se dieron entre las dos variables que luego sirvieron como insumo para fundamentar el modelo propuesto. Los resultados de este análisis fueron presentados por medio de tablas y gráficos teniendo en cuenta las dimensiones, indicadores y variables en estudio.

## 2. Resultados

En el diagnóstico de la situación actual para intercambiar información académica entre la UNPRG y el CPU, se encuestó al personal administrativo vinculado con el área de tecnologías informáticas de la UNPRG, obteniendo los siguientes resultados descriptivos.

DOI: http://dx.doi.org/10.46925//rdluz.32.21

**Tabla 1**. Nivel de conexión de la red para intercambiar información académica

| Rango | Nivel de conexión | Conexión de la red | |
|---|---|---|---|
| | | Frecuencia (fi) | Porcentaje (%) |
| 85 – 100 | ALTO | 1 | 3.4% |
| 57 – 84 | MEDIO | 12 | 41.4% |
| 0 – 56 | BAJO | 16 | 55.2% |
| TOTAL | | 29 | 100% |

Fuente: Elaboración propia

Como se aprecia en la tabla 1, el 55,2% de los encuestados de la institución, manifiestan que la infraestructura de red no es la óptima, lo que denota que la conexión de la red presenta un nivel Bajo y apenas el 3,4% indica que la conexión de red para intercambiar información académica es Alta.

**Tabla 2.** Nivel de seguridad informática para intercambiar información académica.

| Rango | Nivel de seguridad | Seguridad Informática | |
|---|---|---|---|
| | | Frecuencia (fi) | Porcentaje (%) |
| 85 – 100 | EFICIENTE | 2 | 6.9% |
| 57 – 84 | POCO EFICIENTE | 10 | 34.5% |
| 0 – 56 | DEFICIENTE | 17 | 58.6% |
| TOTAL | | 29 | 100% |

Fuente: Elaboración propia

Tal como se observa en la tabla 2, los encuestados mencionan que al intercambiar información académica, ésta se expone a cualquier tipo de vulnerabilidad, denotándose que el 58,6% lo califican con un nivel Deficiente y tan solo el 6,9% de los encuestados manifiesta que el nivel de seguridad para intercambiar información académica es Eficiente.

En virtud de los resultados y después evaluar el nivel de conexión y el nivel de seguridad de la infraestructura tecnología de la UNPRG, se plantea el siguiente modelo de seguridad informática para VPN que facilite el intercambio de información académica entre dos sitios (ver

DOI: http://dx.doi.org/10.46925//rdluz.32.21

Figura 1). El modelo propuesto consta de dos ejes basados en las dimensiones del objeto de estudio; (a) Gestión de conexión de la red y (b) Gestión de la seguridad informática.

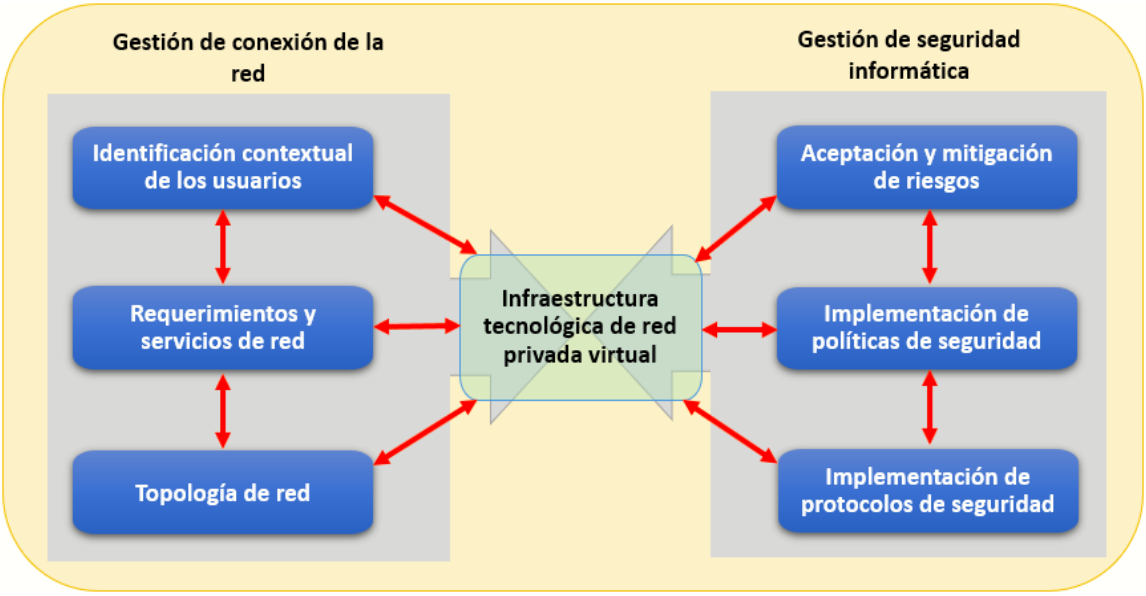


**Figura 1.** *Modelo de seguridad informática para VPN*
Fuente: Elaboración propia

El primer eje describe de manera general los aspectos requeridos para el diseño e implementación de la VPN, y que además incluye las aplicaciones de escritorio, aplicaciones móviles, así como también aplicaciones de software cliente / servidor, todas ellas necesarias para transmitir y recibir información, soportadas bajo la infraestructura de las redes LAN/WAN. Es necesario considerar en este eje los servicios de red, los cuales permitan atender las solicitudes de acceso y procesamiento de la información entre diferentes sitios, tanto locales como remotos. Este eje está conformado por la identificación de usuarios de red, los requerimientos y servicios de red, la topología de red y todos estos elementos confluyen en la infraestructura tecnológica de la VPN.

El segundo eje es el encargado de la gestión de la seguridad informática y contiene los elementos necesarios para aceptar y mitigar riesgos, implementar protocolos y políticas de seguridad. Ambos ejes bifurcan en la infraestructura tecnológica de red privada virtual, constituyendo a su vez el núcleo principal para generar, actualizar, mantener, proteger e intercambiar información entre los sitios de la universidad.

DOI: http://dx.doi.org/10.46925//rdluz.32.21

Para complementar el modelo de seguridad informática, se propone la siguiente topología de red: diagrama de topología física y el diagrama de topología lógica (Cisco Netacad, 2012).

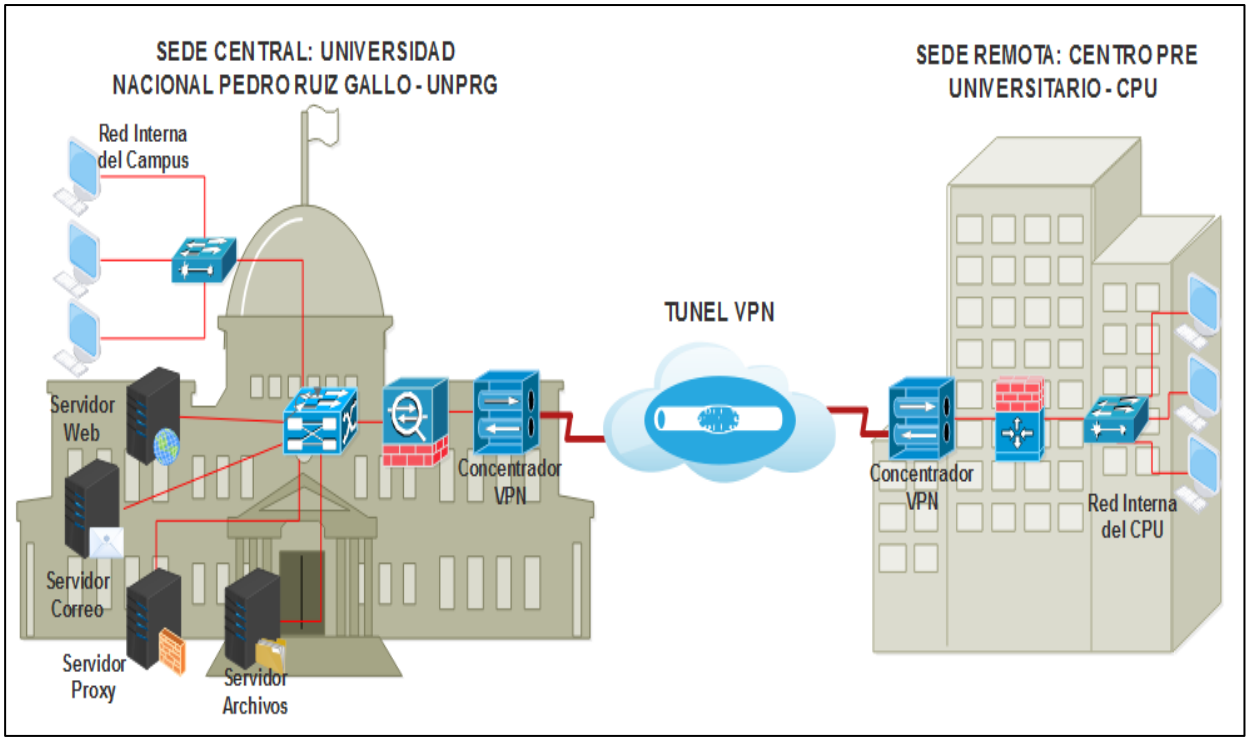


**Figura 2.** *Diagrama de topología física de la red VPN*
Fuente: Elaboración propia

El diagrama de topología física, en el cual se describe la arquitectura física de la red privada virtual y los componentes que la constituyen tales como: routers con capacidad VPN, dispositivos de seguridad multifunción y dispositivos de autenticación y administración central para la agregación y la terminación resistentes de las conexiones VPN, switch multicapa, servidores y dispositivos de usuario final. Véase la figura 2.

Por su parte, el diagrama de topología lógica se encarga de identificar los dispositivos, puertos y esquemas de direccionamiento lógico ipv4. Esta disposición consta de conexiones virtuales entre los nodos de una red. Los protocolos de red asociados definen estas rutas de señales lógicas. Véase figura 3.

DOI: http://dx.doi.org/10.46925//rdluz.32.21

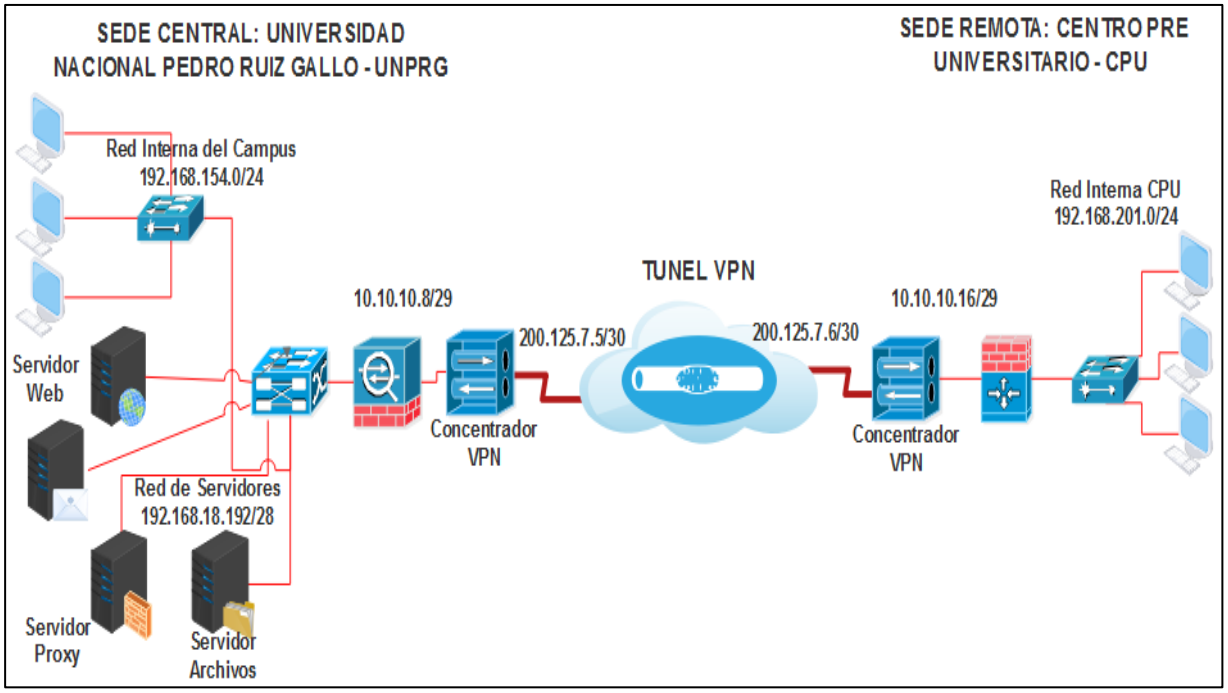


**Figura 3.** *Diagrama de topología logica de la red VPN*
Fuente: Elaboración propia

## 3. Discusión

En este artículo se ha logrado determinar que tanto la seguridad informática como la conexión de la red se encuentran en un nivel bajo (ver tabla 1 y 2), lo que evidencia deficiencias en cuanto al despliegue de la infraestructura tecnológica en la institución universitaria, por lo que al poner en marcha el modelo de seguridad informática para VPN se logrará un diseño eficiente de la red de campus y funcionamiento óptimo de la VPN, garantizando con ello intercambiar información académica de forma segura entre la UNPRG y el CPU de la entidad educativa.

La presente investigación se asemeja a la desarrollado por Jing et al. (2016), dado que se propone un modelo de seguridad informática para VPN, el mismo que describe de manera metódica cada uno de los ejes que lo conforman, incluye la identificación de usuarios, la determinación de requerimientos y servicios hasta la topología requerida para el diseño de red, para luego culminar con gestión de riegos y el manejo de protocolos y políticas de seguridad informática.

DOI: http://dx.doi.org/10.46925//rdluz.32.21

En relación a lo investigado por Wu & Xiao (2019), muestra resultados experimentales a partir de las pruebas de conectividad y seguridad en la red VPN del campus de la Universidad de Beijin, estos resultados beneficiarán a la presente investigación dando pie a que se logre con éxito la implementación del modelo propuesto.

Teniendo como sustento la teoría general de sistemas (De la Peña & Velázquez, 2018), el modelo de seguridad informática para VPN se estructura mediante las dimensiones conexión de la red y seguridad informática, con lo cual se contribuye al diseño de la infraestructura tecnológica de red privada virtual, garantizando la seguridad, escalabilidad y accesibilidad a los recursos y servicios de red y sobre todo certificando la confidencialidad, integridad y disponibilidad de la información.

Es preciso mencionar que las topologías de red descritas en la figura 2 y 3, tributan al modelo propuesto, las cuales guardan relación con la investigación realizada por Zhiyong et al. (2014), en la cual los autores proponen la aplicación de la tecnología VPN en un entorno multi-campus partiendo de una topología lógica y la posterior simulación de la red. Finalmente, concuerda con lo estudiado por Hashiyana et al. (2020) en donde se parte de una topología física y lógica para luego implementarla en un laboratorio de pruebas, logrando de esta forma el diseño e implementación de una VPN en la Universidad de Namibia.

## Conclusiones

En este trabajo se elaboró un modelo de seguridad informática para VPN con la finalidad de intercambiar información académica de manera confiable y segura sobre un medio de conexión pública como internet, entre la UNPRG y el CPU de la organización; para ello se logró determinar que tanto la conexión de la red como la seguridad informática se encuentran en un nivel bajo y deficiente respectivamente.

Lo más importante de la elaboración de este modelo fue el desarrollo de cada uno de los ejes que lo integran, como son la gestión de la seguridad informática y la gestión de conexión de la red, porque con esta propuesta se puede garantizar la seguridad y confiabilidad en el envío de información académica entre los dos sitios de la organización. Lo que más ayudó a elaborar este modelo fue la disposición del personal técnico especialista en tecnologías de la información,

DOI: http://dx.doi.org/10.46925//rdluz.32.21

porque se recolectó información precisa y exacta que contribuyó a construir el modelo propuesto.

La propuesta de la topológica de la red tanto en su diseño físico como en su diseño lógico hace que el modelo se vea fortalecido para su posterior implementación al tener una base técnica y escalable sobre la cual se va a montar la infraestructura de la red VPN, garantizando de esta manera que el intercambio de información pueda ser seguro, confiable y rápido entre la sede principal y el CPU.

La seguridad informática debe ser aplicada tanto desde el interior del campus universitario como desde el exterior; más aún, teniendo en cuenta que muchas de las amenazas provienen desde el interior de las organizaciones, se hace indispensable que los usuarios que no cuentan con suficientes conocimientos en seguridad de la información no sean aislados de la red, sino que por el contrario sean incluidos y capacitados.

## Referencias

Altamirano, M. D. L. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Avances*, 21 (2), 248–263. http://www.ciget.pinar.cu/ojs/index.php/publicaciones/article/view/440

Amankwa, E., Loock, M., & Kritzinger, E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014), 248–252. https://doi.org/10.1109/ICITST.2014.7038814

Aung, S. T., & Thein, T. (2020). Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks. 2020 IEEE Conference on Computer Applications(ICCA), 1–5. https://doi.org/10.1109/ICCA49400.2020.9022848

Bernal, C. A. (2010). Metodología de la Investigación. In Pearson Educación (Tercera). Pearson Educacion.

Cisco Netacad. (2012). 4.4.1.2 Topologías física y lógica. Cisco Networking Academy. http://itroque.edu.mx/cisco/cisco1/course/module4/4.4.1.2/4.4.1.2.html

De la Peña, G., & Velázquez, R. M. (2018). Algunas reflexiones sobre la teoría general de sistemas y el enfoque sistémico en las investigaciones científicas. Revista Cubana de Educación Superior, 37(2), 31–44.

Deloitte. (2016). La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información. https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte 2016 Cyber Risk Information Security Study - Latinoamérica - Resultados Generales vf (Perú).pdf

Deshmukh, D., & Iyer, B. (2017). Design of IPSec virtual private network for remote access. 2017 International Conference on Computing, Communication and Automation (ICCCA), 716–719. https://doi.org/10.1109/CCAA.2017.8229894

Esparza, D. E. I., Diaz, F. J., Echeverria, T. K. S., Hidrobo, S. R. A., Villavicencio, D. A. L., & Ordonez, A. R. (2020). Information security issues in educational institutions. 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), June, 1–7. https://doi.org/10.23919/CISTI49556.2020.9141014

Estatuto UNPRG. (2017). Estatuto Universidad Nacional Pedro Ruiz Gallo. In Universidad Nacional Pedro Ruiz Gallo. Universidad Nacional Pedro Ruiz Gallo. http://www.unprg.edu.pe/univ/portal/documentos_s/7. ESTATUTO ACTUALIZADO 2019 DE LA UNPRG.pdf

Hashiyana, V., Haiduwa, T., Suresh, N., & Bratha, A. (2020). Design and Implementation of an IPSec Virtual Private Network : A Case Study at the University of Namibia. 2020 IST-Africa Conference (IST-Africa), 1–6. https://www.researchgate.net/profile/Valerianus_Hashiyana/publication/344542951_Design_and_Implementation_of_an_IPSec_Virtual_Private_Network_A_Case_Study_at_the_University_of_Namibia/links/5f7f097ba6fdccfd7b4f9bd2/Design-and-Implementation-of-an-IPSec-Virtual-Private-Network-A-Case-Study-at-the-University-of-Namibia.pdf

Hernández-Sampieri, R., Fernández, C., & Baptista, P. (2018). Metodología de la Investigación. In Mc Graw Hill (Sexta). Mc Graw Hill.

Jing, S., Qi, Q., Sun, R., & Li, Q. (2016). Study on VPN Solution Based on Multi-campus Network. 2016 8th International Conference on Information Technology in Medicine and Education (ITME), 777–780. https://doi.org/10.1109/ITME.2016.0180

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. Journal of Information Security and Applications, 35, 128–137. https://doi.org/10.1016/j.jisa.2017.06.006

Li yong. (2015). Analysis of network connectivity probability on damage probability. 2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 1056–1059. https://doi.org/10.1109/IAEAC.2015.7428719

Ponemon Institute. (2018). 2018 State of Cybersecurity in Small & Medium Size Businesses. November, 46. https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers and Security, 56, 1–13. https://doi.org/10.1016/j.cose.2015.10.006

Solarte, F. N. J., Enriquez, E. R., & Benavides, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica - ESPOL, 28(5), 497–498. http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. Information Technology and Management, 17(2), 179–186. https://doi.org/10.1007/s10799-015-0252-2

Wu, Z., & Xiao, M. (2019). Performance Evaluation of VPN with Different Network Topologies. 2019 IEEE 2nd International Conference on Electronics Technology (ICET), 51–55. https://doi.org/10.1109/ELTECH.2019.8839611

Zhiyong, L., Bo, Y., Jian, W., & Zhongnan, Z. (2014). Application of VPN Technology in Multi-campus Adult Education Platform. 2014 7th International Conference on Control and Automation, 33–36. https://doi.org/10.1109/CA.2014.15