Designing the VPN with Top-Down to Improve Information Security

Valero Andia Billy Scott, Sanchez Atuncar Giancarlo
Faculty of Systems Engineering, Universidad Cesar Vallejo, Lima, Perú

***Abstract*—In this article, presents a systematic review of virtual private networks (VPNs) and their contribution to improving information security, with a particular focus on the Andia Consortium. It examines how VPN technology, through its ability to provide a secure channel for communication between devices, can protect organizations' valuable digital data against cyber-attacks. Various types of VPN systems, their security strategies, advantages and disadvantages, and their dependence on different protocols and standards are discussed. Additionally, tunneling technology, a key technology in VPN implementation, is explored. Through this study, we seek to identify the benefits and limitations of using VPN to improve information security. This work aims to provide a deeper understanding of how VPNs can be designed from the top down to improve information security in organizations.**

Keywords*—*VPN; cyber-attacks; security information

I. Introduction

Attacks [2] are increasing lately, and it is recommended nowadays to have information security, it is very important to cope in our current era, where technology and information have become increasingly ubiquitous. Protecting our information would be the same as protecting our data from any form or means of unauthorized access, use, disclosure, interruption or destruction, to guarantee the accessibility, reliability and usability of our data of the information. Information security is applied to any type of data, whether it is an email in virtual or physical format, and it applies to all types of companies. (p.1). Imperva (2021) also tells us that the protection of our data is an extensive topic that includes protection against internal and external threats, such as hackers, computer viruses, natural disasters and server failures. The stability of our data also means that our privacy will be protected from third parties, since personal and financial information can be stolen and used fraudulently. In general, information security is essential to ensure a sequence of elements and the reputation of organizations in today's world (p.1) [31].

Currently [3] the increase in Information and communication technologies (TIC) has caused a growth in the amount of data that is sent through the Internet, which in turn has increased concern about the security of this information. One of the most effective ways to ensure online data protection [1] through the VPN method that is carried out by computers that allows a secure extension of the local area network, which allows data encryption and connection to internet through secure servers (p.3).

In line with this need, [4] businesses and government organizations have started implementing VPN solutions in order to ensure online data security. For example, [33] in a recent research study carried out by Cid-Fuentes et al., it was found that the use of VPN is an effective strategy to protect online information in Spanish companies in various areas of the sector, such as education, also the area health, and finances. Designing a VPN can be a complex process that requires consideration of multiple factors, such as the choice of encryption protocols and server configuration. In this sense, the Top-Down methodology has been proposed as an effective way to approach the design of security networks, by allowing the risks and needs of this security to be detected and identified before the implementation of the solution.

In our country, [5] information security became a very recent topic of concern. Technology advances at very rapid pace, thus becoming more important for our environment, making it much more difficult to find correct ways to defend ourselves and, in turn, the consortium's information. Given that our network is becoming larger and more complex, and with the emergence of the Internet of Things, it is necessary to look for innovative alternatives and protect our information data. Therefore, the use of a VPN could provide an effective solution to ensure that we provide a confidential and complete service in the company [27].

According to the Ministry of Labor and Employment Promotion (MTPE), it reported 226 thousand formal workers under the modality of teleworking or remote work, which represents 6.7 percent of formal employees in the private sector, this increases the vulnerability factor for security [17]. Additionally, with the growing number of devices connected to the network, it is difficult to control who accesses confidential information. Therefore, a VPN could allow company employees to access the internal network in a more protected way from any point of internet, while guaranteeing private information along with information security [13].

On the other hand, there is concern in our city about the growing number of cyber-attacks on companies and government organizations. With the emergence of new technologies [6], new forms of cyber-attacks have also appeared, making it necessary to seek effective measures to protect the organization's confidential information. A VPN can provide a more secure solution for the confidentiality and integrity of our company data against possible external threats.

In the current consortium, we are faced with a situation that poses various challenges related to information security [34] and effective communication between headquarters. Defining the problem will allow us to clearly define the key aspects that require attention. Challenges include lack of sensitive information, insecure information due to lack of encryption, poor access control, the need for integrity for our information, and limited data availability. [25] These problems arise from the use of a public cloud with a free account for the exchange of information, as well as the lack of an adequate and secure connection between the consortium's headquarters as seen in Fig. 1. These deficiencies put the confidentiality of important data at risk and may result in the potential disclosure of confidential information.

The relevance of this research lies in its focused approach to analyzing applications and previous studies linked to the implementation of Virtual Private Networks (VPNs) [19] within the scope of information security in business environments. In a context where data protection and cybersecurity stand as critical priorities, this study seeks to justify the urgent need to ensure the integrity and privacy of corporate information. Its primary objective is to delve into the advantages and challenges associated with the adoption of VPNs in today's business landscape [9]. By relying on a robust theoretical framework supported by previous research, it aspires not only to offer specific recommendations for enhancing information security through VPNs but also to establish a solid foundation for future studies in this field, outlining specific areas of focus and potential directions for more effective and adaptable computer security in diverse business contexts.

The fundamental purpose of this study is to critically examine existing research related to the implementation of Virtual Private Networks (VPNs) in the information security process within companies and organizations. This approach aims not only to justify the urgency of safeguarding corporate data but also to deeply comprehend the inherent benefits and obstacles associated with VPN adoption in business environments [7]. With a rigorous approach supported by a review of specialized literature, the intention is to provide substantial recommendations for enhancing information protection using VPNs, while also laying the groundwork for future research that explores areas for improvement and development in enterprise computer security.

In this paper, we explore the potential of Virtual Private Networks (VPNs) as a viable solution to address the growing information security [39] concerns faced by the consortium. Through a comprehensive analysis of existing research and a thorough assessment of the advantages and challenges associated with VPN implementation, this study aims to provide valuable insights and recommendations. In particular, we will examine how VPNs can mitigate the specific challenges faced by the consortium, such as the lack of encryption and insecure information exchange. Additionally, we will discuss best practices for the effective adoption of VPNs in a business environment. Ultimately, this study aspires to contribute to the development of a secure and efficient information sharing system within the consortium, thereby strengthening its stance against evolving cyber threats.

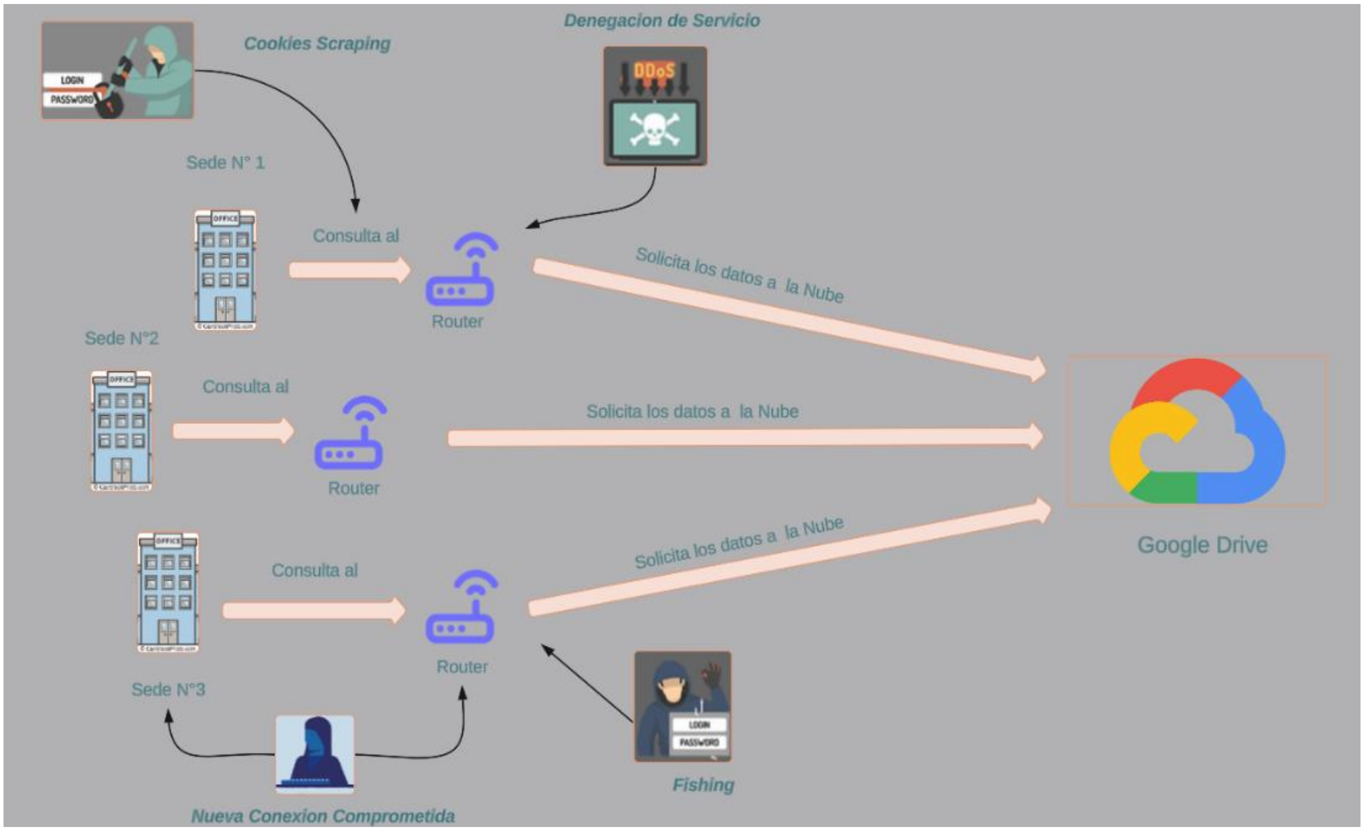


Fig. 1. Graphic Representation of the current situation of the consortium.

II. Methodology

First, this section compiles various research conducted in recent years on the application of VPN and security information.

There are many works or studies carried out on the topic of information security, [8] in the search for information, research similar to the title was found, in the national environment the research of Lazarte and Silva, 2022, in their proposal Creating a VPN using open-source software This report provides valuable information on how to implement a VPN under open-source software to improve information security in a specific area. The methodology that was used was the Top-Down Network Design methodology for the implementation of the project to deploy a Virtual Private Network using free software solutions. This methodology consists of four phases: Conduct a thorough analysis of the requirements, develop a detailed logical design, develop a corresponding physical design and perform rigorous testing, effective optimization and complete documentation of the implementation (p.15) [36].

In another study [10] it is proposed to create a framework to use a virtual network protocol with free software and increase Internet bandwidth. Based on the Cisco PPDIOO (Prepare, Plan, Design, Implement Operate and Optimize) methodology, the V2RAY platform architecture is implemented on AWS and ORACLE clouds. The results of the evaluations before and after using the solution showed significant improvements in several metrics. In particular, the download speed increased by 26.4%, the upload speed increased by 79.5%, and the response time increased by One Hundred per cent. In addition, a dropout rate of One Hundred Percent was recorded, which was also considered significant with a p-value < 0.05 for its indicators (p.12).

It was also found in the work in 2021, [11] in its title VPN and its implementation with PPDIOO to improve computer security, the implementation of a VPN is proposed to make improvements, in information security in the company network. The research is based on a sample of 30 processes related to computer security, using observation sheets to collect data. [23] A quantitative approach and a pure experimental design were used, applying statistical tests to contrast the hypotheses. The results obtained show a significant decrease in the number of incidents reported by users, a reduction in the number of users connected to the network, a decrease in access time to shared folders, and an increase in the level of user satisfaction. the users.

In the work where VPN is implemented [12] and thus improves information security, the main objective was to improve network services through the implementation of a VPN in the educational institution. This research used a quantitative approach, with a pre-experimental design. The sample consisted of 30 participants, and information was collected through questionnaires related to VPN and also information security. The results revealed that VPN implementation was at a medium level, while the dependent variable showed a trend towards the high level with much of the medium level. When contrasting VPN implementation with information security, a significant influence was found between both variables. That is, by increasing the implementation of the VPN in the Public Military Educational Institution Colegio Militar Francisco Bolognesi, a direct correlation could be verified with the improvement of information security. In contrast, a decline in VPN adoption resulted in a decline in data security. These findings highlight the importance of using a VPN as a key and important factor towards information security.

The main purpose [14] was to implement a risk system in the IT area in a strategic plan, so that information security improves in the advertising company. The focus was on the organization's ability to manage risks and prevent potential cyber-attacks and inappropriate manipulations of information. Adequate levels of integrity, privacy and accessibility to the continuity of information were established. When this process was carried out, it was decided to use the Magerit methodology, which made it possible to carry out an exhaustive analysis of the risks present in the organization and obtain specific responses to said risks. These responses were used to implement some solutions in enterprise information security management (p.10).

Similarly for his research, [15] demonstrates that the purpose of implementing ISMS is to safeguard information assets that are fundamental to the company's objectives. In achieving this, it was decided to use the The Deming approach, or the PDCA (Plan-Do-Check-Act) approach, is highly recommended by the ISO 27001 standard for ISMS (Information Security Management System). The result obtained is the minimization of the risks associated with the risks and weaknesses that affect data, documents, systems, technological infrastructure of the Clinic MEDCAM Perú S.A.C. [28], as well as the guarantee of privacy, accessibility and consistency of that information. In conclusion, the most important benefit is to ensure the security of information resources to achieve business objectives (p.8).

Likewise, for Luna [16] its objective is to develop a tool, with a solid base of profitability and usefulness, to establish a remote access VPN connection or link using MIKROTIK equipment that prioritizes the confidentiality of the transfer of information from point A. to point B, preventing unauthorized Internet Points from violating or capturing packets in the traffic and stealing the information sent and received through this VPN, advantageously improving the performance of the network infrastructure, increasing the performance of the packets sent, in addition to demonstrate that resources are used less and RAM workloads are used MIKOTRIK VPN, not like other remote agents with greater memory consumption (p.8).

Also in Ecuador [18], in his work on Security Management aligned with the 27001 standard, he comments that the main objective is to design a methodology that allows the IS to be efficiently and adequately managed, based on the ISO 27001 standard and also the security frameworks. cybersecurity established in ISO/IEC 27032. This methodology focuses on analyzing security gaps in IS, in order to guarantee its protection effectively. It is important to highlight the close relationship between established frameworks and ISO standards. 27001[29] and ISO 27032, which focus on ISMS and cybersecurity. What is proposed is that the developed methodology has the capacity to identify the processes, standards and protocols that are involved in the IS at different management levels.

It is also said that the Internet, as a communication platform, plays a fundamental role in today's society. These technologies allow sensitive information, classified as secret or confidential, to be transmitted over insecure networks by establishing communication tunnels protected by cryptographic methods.

III. Results

To carry out the current research, the methodology known as Top-Down Network Design seen graphically in Fig. 2, will be used, which has proven its effectiveness in various fields of Engineering. The top-down methodology is important in the industry because it allows designers to understand the system as a whole before starting to design the details. This helps ensure that the system is consistent and working correctly.

It is crucial to highlight that the Top-Down Network Design methodology provides valuable benefits to organizations that adopt it. These benefits encompass improved communication between current and future designers; greater quality control by allowing early identification of defects in the initial stages of design, when their correction is easier and cheaper; increasing designer efficiency by reorganizing design tasks and executing them in parallel, rather than relying on linear sequences; as well as reducing the need for extensive verification of the final design state Phases of the Top-Down Network Design Methodology in Table I.

The methodology has four phases that help the creation and implementation of the

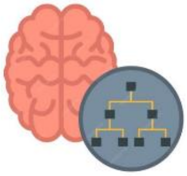
Phase 1: Analyze requirements.

Phase 2: Develop Logical Design.

Phase 3: Develop Physical Design.

Phase 4: Test, optimize and document design.

TABLE I. Methodology Top-Down

Phase	**Process**	**Activities**
Phase 1 Analyze Requirements	Analyze the objectives and limitations of the company	*- Definition of Goals* *-Specify Objectives* *-Current situation of the company*
	Analyze the objectives and technical limitations	
	Characterize the existing network	
	Characterize network traffic	
Phase 2 ***Develop Logical Design*** 	Design a network topology	*-Design a network topology* *-Design addressing models* *-Select switching and routing protocols* *-Design network security strategies* *-Design network management strategies*
	Design addressing and naming models	
	Select Switching and Routing protocols	
	Develop security strategies	
	Develop strategies for network maintenance	
FASE 3 Develop Physical Design	Select technologies and devices for networks	*-Technical hardware details.* *-Technical connection details* *-Computer configuration and your Ruijie Cloud*
FASE 4 Test, optimize and document ***design***	Test network design	*-Configure VPN policies* *-Test the design between the venues* *-Configure shared folders on the VPN network*
	Optimize network design	
	Document network design	

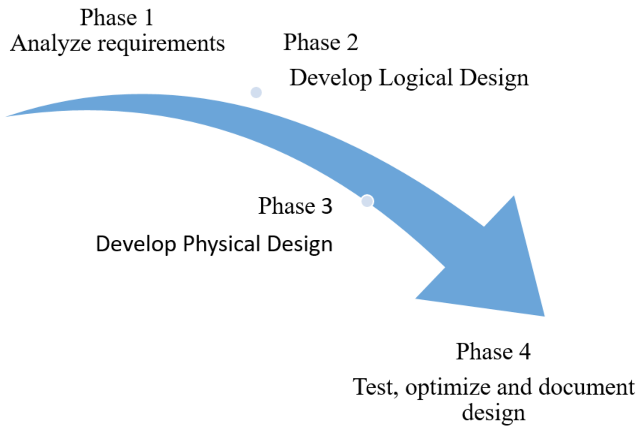


Fig. 2. Methodology top-down.

Phase 1: Analyze requirements

a) Activity 1: Definition of Goals

Through a series of discussions and meetings with department leaders, we collaboratively identified key factors that contribute to the following overall goals:

- The Andia Consortium wants to expand its presence in the real estate market, both nationally and internationally. To do this, it plans to open new offices in other countries and expand its portfolio of products and services. It also strives to offer its clients a wide range of real estate products and services, from the purchase and sale of properties to rental management and home construction. In the same way, it wants to be recognized as a leading company in the real estate sector. To this end, it is committed to offering a high-quality service and being at the forefront of the latest market trends.

- The Andia consortium currently needs technological tools such as electronic invoices, access to a secure intranet, and information sharing to be able to complete business activities within the company. This need comes from the advancement of technology, it is inevitable not to work with current technology and in the case of the consortium having three isolated offices, a network that integrates the branches is necessary, for this reason it is desired to implement a secure network complying with the rule of the CIA triad (Confidentiality, Integrity and Availability).

b) Activity 2: Targeting of Objectives

Having identified the critical issues facing the Andia Consortium, we can now define specific and measurable objectives for the project. These objectives will address the identified problems and contribute to achieving the overall goals:

- Improve information security: The consortium wants to protect your data from loss, disclosure or unauthorized access. To do this, it will implement a role-based access control system, an auditing system and a secure and efficient network infrastructure.

- Improve the efficiency of operations: The consortium wants to streamline its processes and procedures to reduce costs and improve productivity. To do this, you will centralize your data in a single repository, standardize your processes and procedures, and automate repetitive tasks.

- Improve the customer experience: The consortium wants to offer a high-quality and personalized service to its customers. To do this, it will implement a system defined for networks or centralized cloud, where it can monitor clients, having a specific solution for each client.

c) Activity 3: Current Situation of the Company

The Andia Consortium, a real estate company with multiple branches in Lima, currently utilizes an internal wired network to connect its offices and accesses external resources through a separate internet service. A thorough assessment of the existing network infrastructure, including its topology, addressing scheme, equipment capabilities, and security posture, is crucial for the design process:

- Current situation of the Andia Consortium network is made up of the following elements: Routers, switches, wireless PCI cards, wireless routers, computers and laptops. An internal network that is responsible for all the Consortium's traffic at each headquarters independently. There is also an Internet service through which they access external resources and communicate between branches.

- The current problems of the Consortium are the lack of confidentiality by not having secure policies, the data traveling freely without any type of security, it is also not protected against alterations since it does not have an audit system or log records, and availability in case the network fails and there is no backup.

Phase 2: Develop Logical Design

a) Activity 1 Design a Network Topology

A star network (see Fig. 3) topology will be used for the VPN design. This structure allows all devices to interconnect with each other centrally, resembling a local area network (LAN). This configuration offers efficient communication and simplified network management.

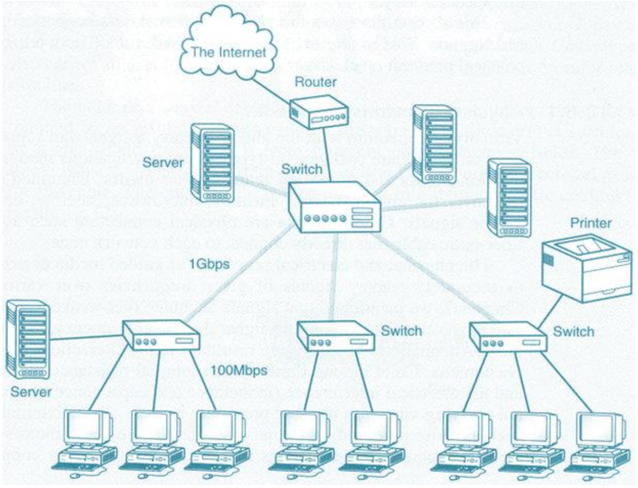


Fig. 3. Star topology.

b) Activity 2 Design Addressing and Naming Models

The Ruijie Network R105G Router will be used to establish the addressing model. We will implement static routing, which will be manually configured in the Ruijie Cloud settings to manage the router. This approach provides granular control over network traffic flow. It also provides granular control over network traffic flow as seen in Table II.

TABLE II. ADDRESSING TABLE

Dispositivo	Interfaz	IP
Router1	Vlan 10 (Vlan OP)	192.168.10.1
PC10	NIC	192.168.10.10
Router 2	Vlan 20 (Vlan S.C.)	192.168.20.1
PC20	NIC	192.168.20.10
Router 3	Vlan 30 (Vlan Mochicas)	192.168.30.1
PC30	NIC	192.168.30.10
Router 1,2 y 3	Vlan 50 (Vlan administration)	192.168.50.1
	Vlan 80 (Vlan IoT)	192.168.80.1
	Vlan 90 (Vlan Guest)	192.168.90.1

c) Activity 3 Select Switching and Routing Protocols

The Ruijie Network Router's supported switching and routing protocols will be carefully selected as seen in Table III. While the final decision will depend on specific network requirements, static routing with inter-branch connections is a potential option for this design.

TABLE III. SWITCHING AND ROUTING PROTOCOLS

Tecnology	Content	Service
Ipsec Protocol	ESP, AH	
Encryption	DES , 3DES, AES	Privateness
Data digest	MD5, SHA	Integrity
Identity Authentication	RSA, Pre-shared Key	Authenticity
Key Exchange	DH1, DH2, DH5, DH14	Key Security

d) Activity 4 Develop network security strategies

Leveraging the security features offered by the Ruijie Router, we will design a comprehensive security strategy for the VPN network. This strategy may include functionalities such as traffic analysis, access control, encryption, application protection, and flow control.

e) Activity 5 Develop network management strategies

The Ruijie Cloud platform offers a robust set of network management tools. We will utilize this platform for tasks such as policy management, device management, user management, application management, and security management. This centralized approach simplifies network administration and facilitates troubleshooting.

Phase 3: Develop Physical Design

a) Activity 1 Technical details of the Hardware

- A detailed breakdown of the hardware components to be used in the physical design is provided in Table IV. This breakdown should include specifications for each piece of equipment, such as the Ruijie Router model, switch model, and any additional hardware required for the network.

TABLE IV. HARDWARE DETAILS (TECHNICAL)

Characteristic	Description
Modelo	RG-EG105 P
Network Interface	5 puertos Base-T 10/100/1000
Certificated	CE, ROHS
RAM	DDRIII de 128 MB
Port WAN	2 puertos Base-T 10/100/1000
Bandwitch	600Mbps
Storage	Flash de 16 MB
PoE	802.3af/at en LAN1-4

b) Activity 2 Technical connection details

The current internet connection details for the Andia Consortium are outlined:

- Connection Type: HFC Fiber
- Bandwidth: 100 Mbps
- Handoff Device: UBEE device
- Network Distribution and Administration: Ruijie Router

- Table V can be included to visually represent the physical connection between the UBEE device, Ruijie Router, and other network components.

TABLE V. PHYSICAL CONNECTION

TYPE	BRAND	MODEL	TOTAL
Router	Ubee	Docsis 3.0	1
Router	Ruijie	RG105 P	3
Switch	TPLink	TL SG1016D	1
Access Point	Ruijie	RAP2260G	1
Computer	Intel	I3 8000	1
Computer	Intel	Core duo	12

c) Configuration of the device and its Ruijie Cloud

Then proceed to configure Ruijie Cloud.

- This activity should focus on the configuration steps for Ruijie Cloud and the Ruijie Router, not individual computers. Here's a revised explanation:
- Access the Ruijie Cloud platform at: https://cloud-la.ruijienetworks.com/
- Create an account and log in to the Ruijie controller.
- Once logged in, configure the following network settings within Ruijie Cloud (see Fig. 4):
  - IP addresses and static routes
  - VLANs
  - VPN configuration for enhanced information security

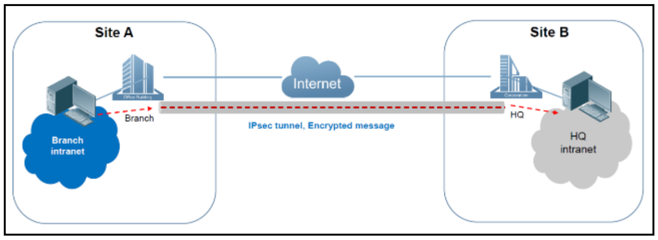
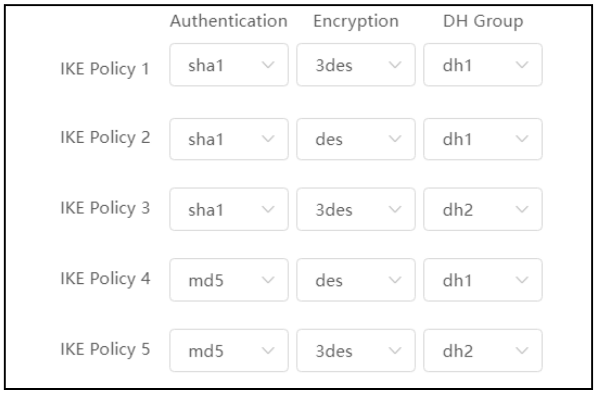


Fig. 4. Topology Ruijie cloud.

Phase 4: Test, optimize and document design.

a) Activity 1 Configure VPN policies

- This activity involves defining the guidelines for secure VPN access. Details regarding user authentication methods, encryption protocols, and access controls should be outlined in Fig. 5.



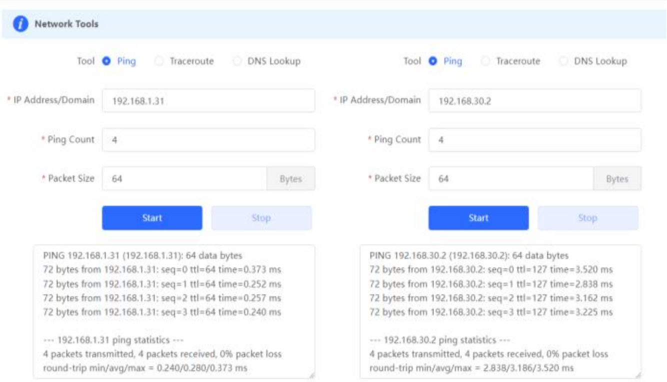
	Authentication	Encryption	DH Group
IKE Policy 1	sha1	3des	dh1
IKE Policy 2	sha1	des	dh1
IKE Policy 3	sha1	3des	dh2
IKE Policy 4	md5	des	dh1
IKE Policy 5	md5	3des	dh2

Fig. 5. Security VPN IPSec.

b) Activity 2 Test the design between sites

The functionality and performance of the VPN connection across different locations should be thoroughly validated. Fig. 5 can be used to illustrate this process.

- Consider revising the explanation to state: "Fig. 6 demonstrates a ping test conducted from the Ruijie Cloud console. The successful pings to both addresses (192.168.1.31 and 192.168.30.2) indicate connectivity between the routers at different sites, verifying communication between subnets and gateways."



Tool ● Ping ○ Traceroute ○ DNS Lookup

* IP Address/Domain: 192.168.1.31

* Ping Count: 4

* Packet Size: 64 Bytes

```
PING 192.168.1.31 (192.168.1.31): 64 data bytes
72 bytes from 192.168.1.31: seq=0 ttl=64 time=0.373 ms
72 bytes from 192.168.1.31: seq=1 ttl=64 time=0.252 ms
72 bytes from 192.168.1.31: seq=2 ttl=64 time=0.257 ms
72 bytes from 192.168.1.31: seq=3 ttl=64 time=0.240 ms

--- 192.168.1.31 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.240/0.280/0.373 ms
```

Tool ● Ping ○ Traceroute ○ DNS Lookup

* IP Address/Domain: 192.168.30.2

* Ping Count: 4

* Packet Size: 64 Bytes

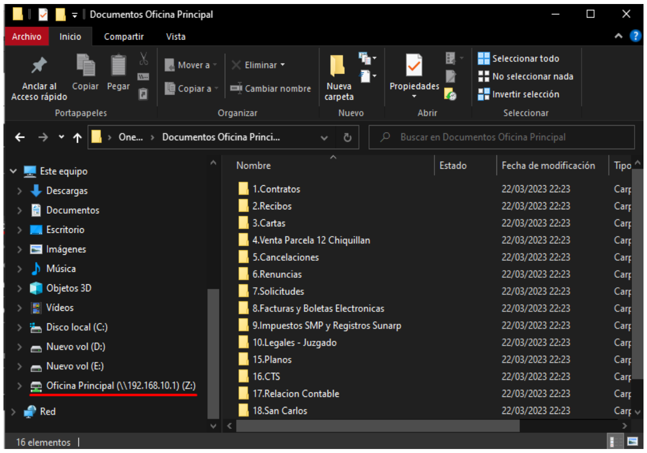
```
PING 192.168.30.2 (192.168.30.2): 64 data bytes
72 bytes from 192.168.30.2: seq=0 ttl=127 time=3.520 ms
72 bytes from 192.168.30.2: seq=1 ttl=127 time=2.838 ms
72 bytes from 192.168.30.2: seq=2 ttl=127 time=3.162 ms
72 bytes from 192.168.30.2: seq=3 ttl=127 time=3.225 ms

--- 192.168.30.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.838/3.186/3.520 ms
```

Fig. 6. Demonstration of successful connection.

c) Activity 3 Configure shared folders on the VPN network

This activity explains how shared folders will be accessed within the VPN environment. Here's a revised explanation:

- To configure shared resources on the VPN, the default storage location where all files are saved needs to be identified.
- Assuming successful VPN configuration, access the network drive locally using the appropriate network address.
- Finally, establish a connection between the storage server and the desired computer by generating and pinning a shortcut as seen in Fig. 7.



Nombre	Estado	Fecha de modificación	Tipo
1.Contratos		22/03/2023 22:23	Carp
2.Recibos		22/03/2023 22:23	Carp
3.Cartas		22/03/2023 22:23	Carp
4.Venta Parcela 12 Chiquillan		22/03/2023 22:23	Carp
5.Cancelaciones		22/03/2023 22:23	Carp
6.Renuncias		22/03/2023 22:23	Carp
7.Solicitudes		22/03/2023 22:23	Carp
8.Facturas y Boletas Electronicas		22/03/2023 22:23	Carp
9.Impuestos SMP y Registros Sunarp		22/03/2023 22:23	Carp
10.Legales - Juzgado		22/03/2023 22:23	Carp
15.Planos		22/03/2023 22:23	Carp
16.CTS		22/03/2023 22:23	Carp
17.Relacion Contable		22/03/2023 22:23	Carp
18.San Carlos		22/03/2023 22:23	Carp

Fig. 7. Connection Established.

IV. DISCUSSION

The comprehensive evaluation of implementing a Virtual Private Network (VPN) in Consorcio Andia revealed significant improvements in the security, integrity, and availability of business information. These improvements can be attributed to the specific characteristics of the VPN application, as well as its alignment with the previously established research objectives.

In terms of information security, the results indicated a substantial advancement after implementing the VPN based on the Top-Down methodology. This not only validated the alternate hypothesis posed in this study but also significantly supported the previous research conducted by Pablo Huanca on information security in a different business context [26].

Furthermore, [40] comparison with Alvarado Sánchez's 2018 study on information management in corporate networks highlighted a notable increase in user approval regarding data protection following the VPN implementation in Consorcio Andia. These findings further underscore the significant enhancement in data protection, emphasizing the importance and effectiveness of VPN as an information protection tool.

Regarding information integrity, both our results and the findings from Huanca [18] suggested a positive impact of the VPN in this aspect. The gathered data exhibited considerable variability between medium and high levels of acceptance regarding information integrity, emphasizing its crucial role in data security within business environments.

Finally, information availability experienced notable improvements with the introduction of the VPN. Despite the study by Julio Morales indicating an increase in the time required to access shared folders with the VPN, our analysis revealed a significant reduction in access time, indicating a substantial improvement in information accessibility within Consorcio Andia. [38].

To validate the security posture of the designed VPN network, we will leverage the CIS (Cybersecurity Infrastructure Survey) Controls framework [37] from the Cybersecurity & Infrastructure Security Agency (CISA). We have mapped specific CIS Controls to our security strategies, such as access control through user authentication and encryption protocols. Utilizing the CIS Controls self-assessment tool, we will evaluate the effectiveness of our design in meeting these critical security practices. The findings from this assessment will be documented and any identified gaps will be addressed through adjustments to the VPN configuration or implementation of additional security measures."

Several studies have explored secure VPN design for multi-branch networks. Lazarte and Silva 2022, in their proposal creating a VPN using open-source software, utilized a centralized management platform for VPN configuration, similar to our approach using SDN. However, their design focused on OpenVPN software for encryption, while our solution leverages the built-in security features of the Ruijie Router. This simplifies implementation and potentially reduces management overhead [30].

V. Conclusion

After exhaustively reviewing studies related to the implementation of Virtual Private Network (VPN) in Consorcio Andia, a thorough analysis of a limited yet significant number of sources is observed. Among the 42 sources analyzed, 5 articles (12.67%) from Science Direct, 11 (20%) from Redalyc, 20 (32%) from IEEE Xplore conferences, and 6 (38.33%) from WebOfScience were selected, encompassing both articles and conferences. These studies offer an overview of the applications, advantages, and challenges surrounding VPNs within the specific context of Consorcio Andia [32].

The evaluation of these existing studies emphasizes the critical importance of VPNs in safeguarding and protecting business information. These analyses span from the technical implementation of VPNs to the security protocols used and their influence on information management. They also highlight how VPNs have evolved and their impact on remote access processes and data security, especially in special situations such as the crisis generated by the COVID-19 pandemic [20].

For future research, delving deeper into identifying and evaluating the technical requirements necessary to successfully implement VPNs within the specific environment of Consorcio Andia is recommended. This involves considering not only data security and privacy but also their effective integration with existing business management systems and e-commerce platforms [24]. Furthermore, exploring how collaborative strategies between sales and technological development teams influence the design and effectiveness of such systems is advisable [21].

Regarding limitations, challenges in human-machine interaction, technological issues such as natural language processing and personalization, as well as these systems' inability to comprehend complex human situations are identified [22]. Additionally, implementation and maintenance costs, the need for continuous learning, and potential user resistance are considerations. Data security, cultural change, and employee training are also crucial aspects to contemplate [35].

References

[1] Estrada-Esponda, R. D.; Unás-Gómez, J. L.; Flórez-Rincón: O. E. Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. Revista Logos Ciencia & Tecnología 2021, 13 (3), 98-110.

[2] Ahmad, Z.; Ong, T. S.; Liew, T. H.; Norhashim, M: Security monitoring and information security assurance behaviour among employees: An empirical analysis. Inf. Comput. Secur. 2019, 27(2), 165-188.

[3] Al-Fayoumi, M.; Al-Fawa'reh, M.; Nashwan, S.: VPN and Non-VPN Network Traffic Classification Using Time-Related Features. Comput. Mater. Continua 2022, 72(2), 3091-3111.

[4] Andersson, A.; Hedström, K.; Karlsson, F.: Standardizing information security – a structurational analysis. Inf. Manage. 2022, 59(3), 103623.

[5] Banoth, R.; Gugulothu, N.; Godishala, A.: A Comprehensive Guide to Information Security Management and Audit; 1st ed.; CRC Press: Boca Raton, FL, 2023.

[6] Bansode, R.; Girdhar, A. Common Vulnerabilities Exposed in VPN - A Survey. J. Phys. Conf. Ser. 2021, 1714(1), 12045.

[7] Bueno, C.; Mejía, J. Marco de trabajo usando VPN con software libre para mejorar la velocidad de internet en dispositivos móviles con Android. Universidad Cesar Vallejo, Lima, Perú, 2021.

[8] Babativa, C. Investigación Cuantitativa. Fondo editorial Areandino 2017, 1(7), 7-8.

[9] Fernández Bedoya, V. H.: Tipos de justificación en la investigación científica. Espí-ritu Emprendedor TES 2020, 4(3), 65-76.

[10] Heart, T.; O'Reilly, P.; Sammon, D.; O'Donoghue, J.: Bottomup or topdown. J. Syst. Inf. Technol. 2009, 11(3), 244-268.

[11] Kuroda, T.: A Combination Of Raspberry Pi And Softether Vpn For Controlling Research Devices Via The Internet. Jrnl Exper Analysis Behavior 2019, 108, 468-484.

[12] Lacković, D.; Tomić, M.: Performance Analysis Of Virtualized Vpn Endpoints. In: 40th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (Mipro); IEEE: Opatija, 2019, 466-471.

[13] Mendieta, J.; Valencia, J.; Camacho, H.: Diseño y prototipado de Red P2P Definida por Software para Pymes y Trabajo Remoto. Universidad Del Norte, Barranquilla, Colombia, 2020.

[14] Michail, H. E.; Kakarountas, A. P.; Milidonis, A. S.; Goutis, C. E.: A Top-Down Design Methodology for Ultrahigh-Performance Hashing Cores. IEEE Trans. Depend. Secure Comput. 2019, 6(4), 255-268.

[15] MORA, J.: Propuesta metodológica para la gestión de la seguridad de la información alineada a la norma ISO 27001 y ciberseguridad. Pontificia universidad católica del ecuador, Quito, Ecuador, 2021.

[16] Ng, K. C.; Zhang, X.; Thong, J. Y. L.; Tam, K. Y. Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective. J. Manage. Inf. Syst. 2021, 38(3), 732-764.

[17] Peralta, A. R.; Bilous, A.; Flores, C. R.; Bombón, C. F. El Impacto Del Teletrabajo Y La Administración De Empresas. Recimundo, 4(1), 326-335. (2020).

[18] Shaofeng, L.; Chaoping, G.; Weifeng, S.: Design And Implementation Of An Enhanced Vpn Isolation Gateway. In: Int. Conf. Robots & Intell. Syst. (Icris); IEEE: Huai An City, 2019, 82-85. (2017).

[19] Skendzic, S.; Kovacic, B.: Open Source System Openvpn In A Function Of Virtual Private Network. IOP 200, 012065Conf. Ser.: Mater. Sci. Eng.,. (2019).

[20] Zhou, Z.; Huang, T. Open VPN Application in COVID-19 Pandemic. J. Phys. Conf. Ser. 2021, 1865(4), 4(2015).

[21] Bueno, C. y Mejía, J.: Marco de trabajo usando VPN con software libre para mejorar la velocidad de internet en dispositivos móviles con Android. Universidad Cesar Vallejo, Lima, Perú. (2021).

[22] Carlos Babativa: Investigación Cuantitativa, (7)7-8 Fondo editorial Areandino1 (2017).

[23] Carlos Ramos: Diseño de investigación Experimental.Vol. 10 (1) I Revista CienciAmérica. (2021).

[24] Condori-Ojeda, Porfirio: Universo, población y muestra. Curso Taller. https://www.aacademica.org/cporfirio/18.

[25] Conejero Suárez, M., Claver Rabaz, F., Fernández-Echeverría, C., González-Silva, J., & Moreno Arroyo, M. P.: Diseño y validación de un instrumento de observación para valorar la toma de decisiones en la acción de recepción en voleibol. Cultura, Ciencia y Deporte, 12(34),67-75. (2019).

[26] Estrada-Esponda, R. D., Unás-Gómez, J. L., & Flórez-Rincón, O. E.: Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. Revista Logos Ciencia & Tecnología, 13(3), 98-110. (2021).

[27] Fernández Bedoya, V. H.: Tipos de justificación en la investigación científica. Espí-ritu Emprendedor TES, 4(3), 65–76. (2020).

[28] Infantas, S. y Cruz, M.: Diseño E Implementación De Un Sistema De Gestión De Seguridad De La Información Para Proteger los activos de Información De La Clínica Medcam Perú. (Tesis de Ingeniería). Universidad San Martin de Porres, Lima, Perú. (2017).

[29] MORA. J.: Propuesta metodológica para la gestión de la seguridad de la información alineada a la norma ISO 27001 y ciberseguridad (Tesis de ingeniería) Pontificia universidad católica del ecuador, Quito, Ecuador (2021).

[30] Peralta, A. R.; Bilous, A.; Flores, C. R.; Bombón, C. F.: El Impacto Del Teletrabajo Y La Administración De Empresas. Recimundo, 4(1): P. 326-335. (2020).

[31] Perdigón, R.; Pérez, M. T. Análisis holístico del impacto social de los negocios. Revista de Economía y Empresa, 67, 93-112. (2018).

[32] Rojas-Corrales, J. R., & Núñez-Serrano, J. A.: Métodos cuantitativos de investigación. Ediciones Universidad de Salamanca. (2019).

[33] Ruiz López, D., & Fernández García, J. A.: El teletrabajo en tiempos de crisis: un análisis de los determinantes individuales y organizacionales en España. 34(104), 227-244. Revista de Sociología del Trabajo, (2020).

[34] Sánchez de la Vara, J. M., & Espejo-González, L. El uso de VPN en las empresas y su impacto en la seguridad de la información. 6(12), 61-73 Revista S&T,. (2020).

[35] Valencia, R., & Montenegro, M. Métodos de investigación. McGraw-Hill Education (2019).

[36] Rama Bansode and Anup Girdhar, J. Phys.: Conf. Ser. 1714 012045 (2021).

[37] America's Cyber Defense Agency (EE.UU.) Cyber Security Evaluation Tool (CSET). https://www.cisa.gov/.

[38] Al-Fayoumi, M.; Al-Fawa'reh, M.; Nashwan, S.: VPN and Non-VPN Network Traffic Classification Using Time-Related Features. 2, 72 (2), 3091–3111.Comput. Mater. Continua (2022).

[39] Jianyun, C.; Chunyan, L.: Research On Meteorological Information Network Security System Based On Vpn Technology. 2nd International Conference On Electronic Information Technology And Computer Engineering (EITCE), 2019.

[40] TEAS Working Group J. Dong, S. Bryant, Z. Li, T. Miyasaka, Y. Lee.: A Framework for Enhanced Virtual Private Networks (VPN+) Service. Internet-Draft, Huawei, China Mobile, KDDI Corporation, Huawei, November 15, (2019).