International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

# A comparative study of tools for intrusion detection technologies in cyberspace

Francisco Hilario[1], Jorge Mayhuasca[2], Ciro Rodriguez[3], Milner Liendo[4], Giancarlo Sanchez[5]

[1,5]*Universidad César Vallejo, Lima, Perú*
[1,2,3]*Universidad Nacional Federico Villareal, Lima, Perú*
[4]*Universidad Femenina del Sagrado Corazón, Lima, Perú*

*Email: fhilariof@ucvvirtual.edu.pe[1], jmayhuasca@unfv.edu.pe[2], crodriguez@unfv.edu.pe[3], milnerliendoa@unife.pe[4], gsanchezat@ucvvirtual.edu.pe[5]*

***Abstract: The objective of the study was to compare computer security software technologies based on intrusion detection systems in cyberspace in order to provide information to technicians or specialists to opt for the most optimal and quality service for their different criteria and technical qualities, such as: (a) Year of inception, (b) Countries Implemented, (c) Versions, (d) Type of software, (e) Operating System, (f) Cost, (g) Programming Language, (h)Definition, (i) Features and (j) Benefits. These criteria may benefit users to implement these IDS (Snort, Ossec, KFSensor, Spencer) in their projects or entities with hardware that allows them to maintain the care of their network based on rules and alerts that can be managed with levels of complexity depending on the type of malicious attack or anomaly detected and opt for a more optimal solution for the benefit of maintaining information security.***

***Keywords: Intrusion detection tools comparison, intrusion detection systems, IDS, Snort, Ossec, KFSensor, Spencer.***

## 1. INTRODUCTION

Nowadays, cyber-attacks through the network are the most critical drawback of the society. All interconnected networks from the smallest, medium and large, are inconsistent to network threats [1]; [2]. IDSs (intrusion detection systems) are essential to achieve mitigation and identification of potential dangers and malicious attacks in cyberspace [1]; [3]. In addition, computer security is constantly advancing by achieving the development of software to identify anomalies mechanically and in a timely manner inside and outside the network being effective in the technological world [1]; [2]; [3]. On the other hand, malicious attacks maintain and change assiduously, so cyberspace needs a solution based on advanced computer security with technological tools to keep the organization safe and safeguard user information [1]; [4]. Therefore, it is necessary that entities are dedicated to the development of systems for effective and intuitive identification of anomalies in the network [2]; [3].

In addition, many technology groups allow uploading their attack identification data, intrusions, preventions or guidance documents on the network in a public way in order to maintain the research of making software that can identify and study anomalies in the network [5]. In other words, due to how difficult the attacks become because of the changes that these cybercriminals make in order to bypass these detectors and be able to manage to steal important information for the individual or entity, the existing parameter and data identification groups of free access with the aim of modifying, creating and improving systematically and improving

its architecture regularly [1]; [5]; [6]. However, NIDS are oriented to identify malicious operations through the evaluation of data traffic over the network evolving with intrusive and liberal samples [2].

Therefore, [2] developed a high-level algorithm that works on the basis of two phases for handling adverse situations. The first phase uses binary algorithms (b-XGBoost; NN Siamese and DNN) to filter the input data and identify anomalies in the network. After identifying the attacks, the binary algorithm (m-XGBoost) is used to classify them and determine the most appropriate solution [2]. In terms of results, the algorithm showed accuracy, improvement and effectiveness compared to the tests, allowing time and cost optimization [2]. On the other hand, [3] evaluated the taxonomy on techniques (ML, DL) based on the design of intrusion detection systems and a comparison of articles on NIDS is performed to verify criteria such as: (a) strength, (b) trends and (c) proposed solution limitations, (d) trends, (e) evolution of intrusion detection systems in the network, (f) proposed methodology through evaluation metrics and data selection to improve the shortcomings and propose future solutions of NIDS [3]. In summary, there are different options on the benefits and different varieties of functions, algorithms and tests that demonstrate the effectiveness and improvement process that IDSs entail against different malicious attacks that seek to destroy or steal information harming users in general [2]; [3].

## 2. TOOLS AND METHOD

The purpose of this study was to compare free and/or open source and licensed software for the performance evaluation of intrusion detection system techniques through the following indicators: (a) Year of inception, (b) Countries Implemented, (c) Versions, (d) Type of software, (e) Operating System, (f) Cost, (g) Programming Language, (h)Definition, (i) Features and (j) Benefits.

The present study was qualitative since it describes and defines the criteria of Intrusion Detection System performance software.

| Type of Document | Keyword | Quantity |
|---|---|---|
| Scientific Article | Intrusion detection system | 7 |
| Thesis | Firewall, DDos, Cyber attacks | 6 |
| Web Pages | Snort, Ossec, KFSensor, Spencer | 5 |
| Book | Open source and licensed software | 1 |

## 3. RESULTS

Next, the comparative tables of the Free and Licensed Software to evaluate the performance of the Intrusion Detection System techniques are detailed, where the different criteria found to be most influential are compared with the previous studies with the objective of obtaining similarity, difference and/or comparison with the present study. Likewise, by having a free or licensed software structure, it is possible to identify the indicators or criteria selected in the present research. Therefore, it is possible to present, discuss and/or demonstrate the comparison of data obtained in the comparative boxes. Likewise, the results show that the KFSensor software has been in the technological and labor market for many years. In other words, it has an approximation of 27 years of dedication and business use to offer intrusion detection. On the other hand, it was justified that the results of the SNORT, OSSEC and Specter software are

those tools that currently have an appropriate performance for personal and professional use [13]; [15]; [10].

Table 1: Free Software Comparison for Intrusion Detection System

| **INDICATORS** | **SOFTWARE** | |
|---|---|---|
| | SNORT | OSSEC |
| **YEAR OF INITIATION** | The software was founded in 1998 [7]. | The software was founded in 2008 [8]. |
| **COUNTRIES IMPLEMENTED** | Estados Unidos [7] | Holanda, Serbio, China, Alemania, Turco, Italia, Francia, Polaco, Japón, Rusia, España, Portugal [8] |
| **VERSIONS** | V.2.8.6, V.2.9.7.2, V.9.8.0, V.2.9.8.3, V.2.9.11.1, V.2.9.13.0, V.2.9.14.1, V.2.9.15.0, V.2.915.1, V.2.9.16.0, V.2.9.16.0, V.2.9.17.1, V.3.1.0.0 [7] | V.2.9.4, V3.0.0, V3.1.0, V3.2.0, V3.3.0, V3.4.0, V3.5.0, V.3.6.0 [8] |
| **TYPE OF SOFTWARE** | Free software [7] | Free Software [8] |
| **OPERATING SYSTEM** | Windows, Unix y Linux [7] | Linux, OpenBSD, FreeBSD, MacOS, Solaris, Windows, VMWare ESX 3.0,3.5, NetBSD, AIX y HP-UX 11 [8] |
| **COST** | Personal: $ 29.99<br>Business: $ 399 [7] | It is free and open-source software and does not contain a price tag. |
| **PROGRAMMING LANGUAGE** | Language C [7] | Language C [8] |
| **DEFINITION** | The Snort tool is an intrusion detection system that is based on open-source code under the GNU GLP license, likewise, the development plan was developed in the C programming language [7]. | OSSEC software is highly customizable which offers many features to identify, detect and protect network anomalies to maintain security [8]. |
| **CHARACTERISTICS** | The tracker detects anomalies as alerts in a log panel depending on | The intrusion detection system establishes content logs. In addition, the Rootkit and malware detection tool allows network ports |

| | | |
|---|---|---|
| | their critical level in the network [7]. | to be managed upon detection of any intruders. In addition, the performance audit manages file integration monitoring [8]. |
| **BENEFITS** | Because Snort is network connection oriented, some attacks using applications such as sticks can be detected without Snort performing a detection task since it removes and logs those malicious attacks [7]. | The software is centralized on the event logging service and fail2ban active response mechanism, whereby, the system monitors tripwire files. In addition, the logtash alerting and analysis system is one of the benefits mentioned within the OSSEC software [8]. |

Table 2: Comparison of Licensed Software for Intrusion Detection System

| **INDICATORS** | **SOFTWARE** | |
|---|---|---|
| | **KFSensor** | **Specter** |
| **YEAR OF INITIATION** | It was founded in 1994 [9]. | It was founded in 2000 [11]. |
| **COUNTRIES IMPLEMENTED** | Londres e Inglaterra [9] | Suiza [11] |
| **VERSIONS** | V.1.0.2, V.1.0.3, V.1.0.4, V.1.2.0, V.1.3.0, V.1.4.0, V.2.0, V.2.1.4, V.3.0.4, V.4.0.1, V.4.1.0, V.4.2.0, V.4.3.0, V.4.4.0, V.4.5.0, V.4.7.0, V.4.8.0, V.4.9.2, V.4.10.0, V.4.11.4, V.4.12, V.5.0, V.5.1, V.5.2, V.5.3, V.5.4, V.5.4.5, V.5.5.0, V.5.6.0 [9]. | V.7.0, V.6.0.2, V.6.0.1, V.5.5.4, V.5.5.3, V.5.5.2, V.5.5.1, V.5.5.0, V.5.0.3, V.5.0.2, V.5.0.1, V.5.0, V.4.5.0, V.4.0.1, V.4.0.0, V.3.0.3, V.3.0.2, V.3.0.1, V.3.0, V.2.0.2, V.2.0.1, V.2.0, V.1.0.1, V.1.0 [11] |
| **TYPE OF SOFTWARE** | Paid Licensee - Shareware [9]. | Paid Licensee [11] |
| **OPERATING SYSTEM** | Windows [9] | Windows, Linux, Unisys Unix, Irix, Solaris, Tru64, AIX, MacOS, NeXTSTep, FreeBSD [11] |
| **COST** | KFSensor Professional Edition<br>$599<br>KFSensor Enterprise Edition<br>$549 USD<br>KFSensor Subscription<br>$120 USD [9]. | SPECTRE Package<br>$ 899,00<br><br>Additional License<br>$ 399,00<br><br>Upgrade Extension<br>$ 99.00 [11] |
| **PROGRAMMING LANGUAGE** | Wireshark [9] | JavaScript [11] |

| | | |
|---|---|---|
| **DEFINITION** | It is an anomaly detection system that attracts information about attacks, malwares, worms, ransomware in the network, thus, it reports about the system on the basis of vulnerabilities from situation of system services and infection by malicious attacks [10]. | It is a deception system or smart trap, where the Honeypot is based on IDS, sensitive to attackers, where it is offered in having common Internet services such as SMTP, FTP, POP3, HTTP and TELNET where these services comfortably attract attackers, however, these are traps that try to collect information and stop these destructive attacks [10]. |

| **INDICATORS** | **SOFTWARE** | |
|---|---|---|
| | **KFSensor** | **Specter** |
| **CHARACTERISTICS** | It manifests the monitoring of connected ports so it is remotely managed against any malicious attack, protecting against denial of service (DDoS) attacks where data integration is exported in huge logs within the system service to be aware of the different types of attacks that are constantly changing [10]. | The predictable logic of the processor is taken into account. The subsequent difference between cache hits and misses can be reliably measured [12]. |
| **BENEFITS** | KFSensor contains many essential and advanced security features not found in other products so the detections contemplate in having real-time functionality [9]. | Specter has its sensors at the edge of the network where it can immediately detect any suspicious activity and automatically collects data from the attacker. On the other hand, the system is very easy to install and configure so much that it offers the most sophisticated and up-to-date features [11]. |

## 4. DISCUSSION

The licensed software KFSensor was one of the pillars for the development of the intrusion detection prototype (IDS) launching its first software in 1994 in order to detect different attacks [9] this result is similar to the study of [13] when mentioning that the Snort software is one of the oldest and most used systems today for its improvements and security functions more adaptable to the user [13]. Likewise, the Snort open-source software manages to distinguish

the quality of service granted by users by being the system most used by technicians today for its fast manipulation functions, for its integrated tools that have allowed preventing, detecting and monitoring cyber-attacks by increasing security [7]. This result is similar to the research of [14] where they state that Snort and Suricata IDS open source allows solutions with IPV4 and IPV6 protocols maintains an analysis of permissions and anomaly detection through the IPS that allows optimal performance allowing efficiency and effectiveness in different entities [14]. The Specter licensed software is adaptable to different platforms that allows to achieve the quality of its product, these operating software are: (a) Windows, (b) Linux, (c) Unisys Unix, (d) Irix, (e) Solaris, (f) Tru64, (h) AIX, (i) MacOS, (j) NeXTSTep, (k) FreeBSD, this result is different from the study of [15] where it validates that OSSEC software presents the most complete operating systems compared to other software by the adaptability that each user requires, such as: (i) Linux, (ii) OpenBSD, (iii) FreeBSD, (iv) MacOS, (v) Solaris, (vi) Windows, (vii) VMWare ESX 3.0, (viii) NetBSD, (ix) AIX and (x) HP-UX 11 [15]. The open source OSSEC software can adapt to the security requirements based on the broad information criteria including customizable alerting rules and writing lines and programming query (Scripts) to enhance the measures in terms of alerts depending on the critical level of cyber-attack.

Ossec also offers two types of free versions with support: (i) OSSEC +, (ii) OSSEC for Enterprises, these versions are focused on a higher set of users than necessary, apart from having technical support is given the ability to add own rules of the entity in the same way is provided a cloud or server environment and has filters to record different types of attacks [8] this result is similar to the research of Snort open source perfect for users who need to use this tool for a LAN environment since it gives you, guidance, documentation, code and instructions on how to adapt the system platform the network. In addition, Snort offers three types of free versions with support: (a) personal, (b) business, and (c) integrators, which allows a wider range of alerts and a higher margin of alert logs, real-time responses and allows using the name of the system in their business services by opting for the quality of IDS software [7].

On the other hand, the Ossec IDS is programmed in the C language, a type of language very easy to manipulate and very adaptable with the operating systems. Therefore, Ossec is a tool integrated by its functions of event scheduling based on operating systems to validate system files, audit the system against the use of equipment, detect rootkits and generate alerts before dynamic tests [16]. This result is similar to the study of [13], which details that the open-source Snort IDS was developed in C language, so that users can interact with its programming and adapt it to different requirements to provide greater network security. In addition, the programming allows you to analyze network traffic in real time, analyze packets that are sent and received through cyberspace, detect anomalies and generate alerts. The IDS technological tools are used to manage the activities that occur within a network, verify intrusion attempts, manage network traffic to increase rules in order to obtain security between users inside and outside the network [10]. This result is similar to the research of [15] where it details that this system adapts according to the requirements of computer security, since, its multiple configuration options, scripts, rules, modifications and changes of customizable alerts, allows the IDS to perform at its 100%, in addition, to check the integration and reliability of user data, enabling the monitoring of technological hardware (Firewalls) [15].

Next, the characteristic of IDSs makes it possible to recover from possible system crashes, to identify correlations on the network with interconnected devices, to couple easily and simply on the installation systems of these systems and to block any attack of malicious intent on the basis of computer security policy [17]. This result is similar to the study of [18] where it validates that an IDS must have a detection method, must maintain a logging behavior, obtain the location of the attacker and its frequency of use. In addition, it must manage to have

functions such as: (a) behavior, (b) awareness, (c) assets, (d) host parameters, (e) packet transfer, (f) network monitoring, and (g) periodic validations [18]. Finally, the intrusion detection tool Snort has one of the most adaptable services in the face of anomaly detection protocols, in addition, it analyzes the packets through the network, managing rules that will empower the system and/or tool with a series of filters to better perform the functions of the IDS all this in real time, also, it maintains constant updates before different changes in the system by the patterns that are fundamental elements to maintain security in the network [19]. This result is different the study of [18] because it describes that the intrusion detection tool Ossec details of alerts, configurations (Scripts) and centralized management of integrated tools that allows the integration inspection and monitoring log and policies that manage to maintain the security of critical incidents and opt for different solutions that allow alerting about anomalies messages or cyber-attacks that only seek to damage or steal information [18].

Finally, the Snort intrusion detection tool has one of the most adaptable services in the face of anomaly detection protocols, in addition, it analyzes the packets through the network, managing rules that will empower the system and/or tool with a series of filters to better perform the functions of the IDS all this in real time, it also maintains constant updates to different changes in the system by the patterns that are fundamental elements to maintain security in the network [19]. This result is different the study of [15] because it describes that the intrusion detection tool Ossec details of alerts, configurations (Scripts) and centralized management of integrated tools that allows the integration inspection and monitoring log and policies that manage to maintain the security of critical incidents and opt for different solutions that allow alerting about anomalies messages or cyber-attacks that only seek to damage or steal information [15].

The research conclusions were the following: Snort is the free software where it is granted to have a market service with more years of antiquity, for this, it is achieved to have the security functions very adaptable for the users because it allows to have the easiest use to understand at the moment of being able to manipulate the intrusion detection system [13]. On the other hand, Snort is the software that shows a high empathetic level for its processes and development so it is reflected that it is the most optimal type of open-source software because it allows users to interact in a more accurate way and be a better-known software worldwide where it will allow manipulating the detection and monitoring of malicious attacks. In such a way, Ossec software is a platform that allows to have a high level of quality in its products for its didactic functions and to maintain user satisfaction for its different platforms (operating systems) such as: (i) Linux, (ii) OpenBSD, (iii) FreeBSD, (iv) MacOS, (v) Solaris, (vi) Windows, (vii) VMWare ESX 3.0, (viii) NetBSD, (ix) AIX and (x) HP-UX 11 [15].

Next, Snort software proves to maintain a great difference with other IDS, since Snort is a type of open-source software. It also allows Snort software to provide the quality of service, management and ease of use with economic margins, so there are different types of price depending on functions and users: (a) personal, (b) business, and (c) integrators. In this way, it provides a wide range of options for the technician or network administrator when making decisions [7]. On the other hand, Ossec is the software that has a very adaptable language in terms of programming since it is very simple to manipulate by which it is based on the C language and is allowed by the different operating systems, because this type of language is well known and highly demanded in the labor market due to its high competence with different programming languages [16]. In addition, the IDS Ossec before multiple functions stands out its excellent management, meet the requirements of computer security allow different configurations (script) to generate different political alert that can help the entity or the user to detect different attacks in their record and to achieve the integrity and reliability of data before the constant monitoring with interconnected devices [15]. Also, under the characteristics of the

IDS it was possible to maintain adequate control over different anomalies in the network and also a system that identifies malicious devices or attacks detected by the IDS, since this allows to solve and prevent situations of cyber-attacks achieving the IDS to block and alert through a computer and avoid damaging components of a PC's software [16]. Finally, Snort is a very commercial intrusion detection system in the labor market for its adaptability service and performance of functions in real time. In addition, it strengthens against different attacks. Likewise, it is constantly updated in the face of technological changes generating security to the technician or network administrator due to technical changes [19].

The recommendations of this research are the following: This qualitative criterion research can be exercised quantitatively if we denominate criteria with variables, dimensions and indicators that can be measured and evaluated through data collection and statistical tests in order to achieve the hypotheses of the study. To carry out a classification research in order to obtain a classification of intrusion detection system performance evaluation software and to adapt it to more specific environments and allow the management of these network resources and tools. To develop a study using the mixed convergent technique to collect qualitative and quantitative data and make a comparison in search of dissimilarities or differences between the studies to evaluate measurement criteria or information that allows to reach the research objective. It is advisable to conduct longitudinal research to evaluate and validate changes in technological environments for evaluation using IDS software focused on network coverage. To carry out a study of the evolution of IDS systems in order to know the course of development of these systems and the relative changes that took place in the technological path before different types of malicious attacks and to be able to achieve alerts or create parameters that help to optimize processes of intruders. Finally, to be able to increase measurement criteria that can provide a necessary support to the research to allow the administrator or technician to make optimal decisions for projects or entities for the benefit of computer security in need of managing alerts, rules with policies that achieve the effectiveness of the IDS.

**ACKNOWLEDGMENTS**

Our sincere thanks to the authorities and professors of the Universidad Nacional Federico Villarreal, for giving us the opportunity to contribute knowledge through research, thank you very much.

## 4. REFERENCES

[ 1] Muhammad, A. (2021). HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System. *Procesos*, *9*(5), 834.

[ 2] Bedi, P., Gupta, N., & Jindal, V. (2021). I-SiamIDS: an improved Siam-IDS for handling class imbalance in network-based intrusion detection systems. Applied Intelligence, 51(2), 1133-1151.

[ 3] Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150.

[ 4] Singh, V., Sharma, G., Poonia, R. C., Trivedi, N. K., & Raja, L. (2021). Source redundancy management and host intrusion detection in wireless sensor networks. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science), 14(1), 43-47.

[ 5] Lohiya, R., & Thakkar, A. (2021). Intrusion detection using deep neural network with antirectifier layer. In Applied Soft Computing and Communication Networks (pp. 89-105). Springer, Singapore.

[ 6] Lee, S. W., Mohammadi, M., Rashidi, S., Rahmani, A. M., Masdari, M., & Hosseinzadeh, M. (2021). Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review. Journal of Network and Computer Applications, 103111.
[ 7] Snort (2021). Snort Blog.
[ 8] Ossec (2021). Host Intrusion Detection for Everyone.
[ 9] KFSensor (2018). Advanced Windows Honeypot System
[ 10] Enhanced intrusion and insider threat detection for your network.
[ 11] Harlyn, A. (2018). Implementation of Honeypot for the correction of vulnerabilities in the data network of the district municipality of huambos. Thesis (Opting for the Professional Degree of Systems Engineer). Señor de Sipan University. Pimentel: PERU. 204 pp.
[ 12] Specter (2004). SPECTER Year 2000 Product Compliance Statement.
[ 13] Silva, G. (2015). Development of a customized firewall with the option of auto-backup of data to the cloud for SMEs. Thesis (Degree in Computer Science and Multimedia Engineering). International University of Ecuador. Guayaquil: ECUADOR. 195 pp.
[ 14] Nicolaide, W. (2021). Design of an intrusion detection system (IDS) based on neural networks for a software-defined network (SDN) in the faculty of engineering in applied sciences (FICA) of the technical university of the north. Thesis (Degree work prior to obtaining the degree of engineer in electronics and communication networks). Technical University of the North. Ibarra: ECUADOR. 199 pp.
[ 15] Perdigón, R y Orellana, A. (2021). Systems for intrusion detection in data networks of health institutions. *Cuban Journal of Medical Informatics*. 13(2).
[ 16] Marcos, E. (2019). Host Based Intrusion Detection (HIDS) - OSSEC. Thesis (Degree in Computer Engineering). Complutense University of Madrid. Madrid: SPAIN. 112 pp.
[ 17] González, P. (2020). OSSEC: The world of IDS (Intrusion Detection System) and HIDS (Host IDS).
[ 18] Cabrera, H. (2020). *Analysis of the my business system in the first notary's office of Babahoyo.* Thesis (Degree in Systems Engineering). Technical University of Babahoyo. Babahoyo: ECUADOR. 23 pp.
[ 19] Zambrano, A., y Guailacela, F. (2019). Analysis of the efficiency of open-source IDS Suricata and Snort in SMEs. Thesis (Information Technology Audit). Espiritu Santo University. Guayaquil: ECUADOR. 19 pp.
[ 20] Ocampo, C., Castro, Y., Solarte, G. (2017). Intrusion detection system in corporate networks. Scientia et Technica Year XXII. 22(1). ISSN: 0122-170

## Author

**Francisco Manuel Hilario Falcón**

Professor and researcher with experience in various studies and several publications in indexed journals. He is a systems engineer, master in systems engineering, doctor in systems engineering. Member of the College of Engineers of Peru with Reg. CIP No. 99835. Member of the Research group in process of the Community of Knowledge I+D+I+Systems UNFV. Professional experience as Information Technology and Telecommunications Manager, Statistics and Informatics Manager, Information Technology Consultant, IT Project Manager, Virtual Classroom

Administrator, Systems Analyst, Information Technology Specialist. International certifications: Scrum Master Certified (SMC) ID: 712972. Scrum Fundamentals Certified (SFC) ID: 715526. Cybersecurity Management Certification - ISO-27032 N° 200600094-19050005. Information Security Management and Administration Certification - ISO-27001 N° 200700052-19050007. Digital Transformation Certification N° GS3 HHP QYP.

**Author**

**Jorge Víctor Mayhuasca Guerra**

Doctor in Engineering, Master in Systems Engineering, Industrial Engineer, Research Professor, Senior Lecturer appointed to the Faculty of Industrial and Systems Engineering. Director of the Academic Department of Systems Engineering. Director of the Professional School of Industrial Engineering. Member of the Scientific Committee of the School of Industrial and Systems Engineering. President of the quality committee of the Professional School of Systems Engineering, Main Coordinator of the Research group in process of the Community of Knowledge I+D+I+Systems UNFV.

**Author**

**Ciro Rodriguez Rodriguez**

Main teacher and researcher at the Universidad Nacional Mayor de San Marcos of the School of Software Engineering of the Faculty of Systems Engineering and Computer Science in undergraduate of the Universidad Nacional Federico Villarreal in the subjects of System Dynamics, Systems Simulation, Scientific Research, Software Engineering and teacher in Postgraduate Masters and PhD in IT Service Management, Advanced Topics in Engineering, Environmental Informatics, Scientific Research, Software Engineering. Advanced Studies at the Institute of Theoretical Physics of Trieste ICTP Italy and at the USPAS Particle Accelerator School in the United States, IT Development Policy Studies in South Korea. Professor at different.

## Author

**Milner David Liendo Arévalo**

Work experience of more than 23 years in Information Technology and Business Management. Experience as Project Manager and Project Leader guided by the PMI model. Experience in Implementation of IT Best Practices ITIL V04, ISO20000. Experience in Processes and Procedures Implementation with BPM. Experience in Strategic Planning consulting and Business Intelligence management. Expert in IT consulting and support. Experience as University Professor in Undergraduate and Postgraduate and belonging to the scientific community of CONCYTEC. Experience in Smart Cities and Digital Transformation Projects.

## Author

**Giancarlo Sanchez Atuncar**

Systems Engineer graduated from the Universidad César Vallejo, has a Master's Degree in Systems Engineering with mention in Information Technology, has a Diploma in Didactics and Graduate Research, has a second specialty in Information Technology and Communication, at the University Esan. He is currently a PhD Candidate in Systems Engineering at the Universidad Nacional Federico Villarreal, is a Senior Professor at the Universidad Cesar Vallejo, and is a member of the College of Engineers of Peru with recognition for more than 8 years of experience as a Systems Engineer.