

Evaluation of Algorithmic Metrics with A Focus on Server Cyber-Risks

Francisco Hilario, Milner Liendo, Laura Chipana, Cheyer Corpus, Carla Zafra

Universidad César Vallejo, Lima, Perú

fhilariof@ucvvirtual.edu.pe, mliendoare@ucvvirtual.edu.pe, lachipanaro@ucvvirtual.edu.pe, cheyergco@gmail.com, cmzafra@gmail.com

Abstract: The purpose of the study is to evaluate algorithmic metrics focused on cyber risks of servers using: K nearest neighbors, Decision Trees, Naive Bayes and Logistic Regression (machine learning methods that apply classification algorithms), was conducted in order to select the best model to develop predictive standards to mitigate these types of threats. In addition, this research was conducted in order to help public and private entities in the field of cybersecurity to be able to have multiple decisions according to automation, security and process structuring of each algorithm. Another point is, the approach of the study is quantitative, based on a scientific research methodology. Therefore, the results in relation to the test scenario were obtained that each algorithm has demonstrated high performance both in operation and veracity in the face of multiple tests, but Naive Bayes has obtained better results for each metric, likewise, it was determined that such algorithmic parameters help in the analysis and processing of data in order to improve the accuracy of malware threats. In this sense, cybersecurity has been consolidated as a broad term that faces the challenge of strategically balancing multidisciplinary areas that require guidelines, spaces and priorities. As a main recommendation is to implement VPN services to manage the PCs used remotely by users because it maintains a secure data packet channel, they are not easy to breach, in addition, as specialists we must evaluate and validate severely the connection of the tools used by performing a scan for vulnerabilities and constantly employ technology that protects the entity's information.

Keyword: metrics, algorithms, K nearest neighbors, Decision Trees, Naive Bayes, Logistic Regression and cybersecurity

1. Introduction

Technological innovations have provided a high-level development in different areas of networks, communications, computing and cyberspace (Carpio and Miralles, 2021), but with transverse consequences, reaching all social points of the planet, making fast and easy communication its main advantages (Terán Bustamante, Dávila and Castañón, 2019). Therefore, according to (Pinilla, 2021), it turns out that the vast majority of public or private organizations, as well as individuals, depend in one way or another on IT as a key tool to achieve their business objectives or the ability to perform activities in daily life (Carpio and Miralles, 2021; Diaz, Casas and Giráldez, 2019).

Perez (2021) stated that during the COVID-19 health pandemic, a new technological virus has also spread: cyberattack, based on online attacks against information systems, private organizations and state enterprises particularly vulnerable and sensitive felt during this crisis: laboratories, hospitals, scientific research centers, and more, as well as the telecommunications structure and the provision of essential public services (Nagli, 2020; Morales, 2022; Alvarenga and Souza, 2020). Summarizing, the specialist in information theft employs techniques and tools to subtract important information from their target and be able to use it against them or in order to damage the organization to be able to get something in return but employing different varieties of programs and methods to access administrative permission and perform processes that harm the entity, it is for this reason, to implement computer security regulations and specialists in these technological areas (Pozo, 2022; Camargo, 2020).

Cybercrime is an attempt to disable a computer, steal data or use a hacked computer system to carry out additional attacks (Pin and Pinargote, 2022). Cybercriminals use a variety of methods to launch a cyberattack, including malware, phishing, ransomware, man-in-the-middle attacks, and more (Gamboa, 2020). Information system fraud is currently a burning problem in society due to the advancement of technology, due to the anonymity and personal information stored on the internet, catching hackers is increasingly difficult to identify (Silva, 2020; Paredes and Silva, 2021). In addition, among the biggest security problems and challenges faced by companies within their internal network is the entry and propagation of malicious programs or malware through their corporate network, these organizations usually pay special attention to perimeter security, always preparing well in advance of attacks using firewalls (Alvarez and Preciado, 2021; Espinoza, 2020).

Caballero (2020) mentioned that another method is to use zero-day attacks for which anti-malware tools are not prepared and manage to hack the machine (Caballero, 2020; Martínez, 2021). In other words, these attacks have the common goal of obtaining economic benefits through identity theft, theft of banking credentials or sensitive data, followed by ransom demands in cryptocurrency, etc (Silva, 2020; Torres, 2022).

Therefore, the best way to prepare for attacks may be to analyze the organization's infrastructure with security testing (Guaigua, 2021). By delineating the topic towards a more technical environment that deals with device configuration, we can in itself analyze vulnerabilities periodically and identify security red spots (Ameijeiras, Valdés and González, 2021). Therefore, Ovallos et al. (2020) stated that information security has become one of the main issues for any organization. In addition, daily information passing through communication networks is subject to illegal procedures that seek to breach it in one way or another, likewise, risk management allows coordinated activities to direct and control an organization that requires periodic updates on cybercrime and cybersecurity through problem solving and research in an increasing number and due to the current scarcity of scientific literature (Chávez and Moreno, 2021; Vera, 2020).

Finally, this article is developed with the objective of being able to evaluate different algorithmic metrics focused on server cyber risks contemplating multiple functions of algorithms (K nearest neighbors, Decision Trees, Naive Bayes and Logistic Regression) to determine their different processes and the analysis of their performance against computer risk tests (Nunez and Gatica, 2022); Furthermore, to be able to evaluate the effectiveness of its learning method to perform the selection of the best

predictive development model of cyber risk to mitigate these types of threats (Vera, 2020; Yumbo, 2021). To conclude, the general problem was: How do algorithmic metrics influence server cyber risks?

2. Methodology

In this study, bibliographic information from different researchers using the analysis-synthesis method was analyzed, to know the main characteristics and obtain relevant information about penetration testing methods in information systems and servers, the evaluation methods of applied tools were analyzed establishing results through the comparative analysis of such prediction algorithms focused on server cyber risks (Orozco, 2021; Escalante; 2021).

The information risk assessment is performed through questionnaires and interviews to managers corresponding to the development of activities (Martín, 2015). In addition, it is necessary to consider that it is taken into account database and a is necessary of virtual test for the different tests to evaluate the effectiveness of its algorithm structure and prediction to different anomalies (Monterrosso, 2019). Various sources of information such as theses, scientific articles and journals are also used. In this sense, since the research environment requires scientific research, the possible vulnerabilities of the servers are examined and, therefore, it is important to collect reliable and accurate data to determine the extent of the attack produced to the equipment (Rosas and Mesa, 2020).

Analuisa (2022) emphasized a forensic analysis is performed on a non-dedicated file server that, at that time, was used to perform activities other than the



Fig. 1: Vulnerability identification procedure

service provision, such as electronic invoicing, since it was used around a commercial area, in itself, has been discontinued due to the COVID-19 contagion, however, it was abandoned, and when accessing in it, operation problems appear and the need arises to investigate the event to identify and find details of a possible computer attack (Muñoz, 2021; Franco, 2016). For the process of detecting vulnerabilities in the data network, many aspects related to security that are important for its administrators must be addressed, so that the problem can be solved and allow to engage in a complete security protocol for privacy, integrity, accessibility and authenticity (Villacis, 2018; Franco, 2016). In addition, Ramirez (2020) detailed that for this procedure 4 divisions were evaluated:

- Collect data
- Identify insecurities
- Detail solutions to vulnerabilities
- Provide a detailed report of the processes and frameworks carried out.
-

3. Results and Discussion


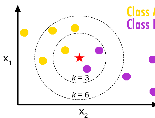
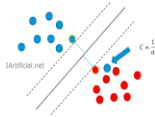


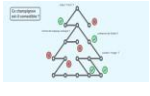
The development of vulnerability analysis involves performing a practical laboratory guide in which system vulnerability operations are performed from a penetration testing perspective to identify key points or errors that may compromise the integrity of the system being evaluated (Bugajski, 2019). The software used in the laboratories can be seen in **Table 1** below.

Table 1: Platforms for the Test environment

Laboratory 1	Laboratory 2	Laboratory 3
Linux Back Track 5	Ubuntu Server 12.04	Ubuntu Server 12.04
Nmap	Nmap	Nmap
BIND9 Server	Linux Back Track 5	Linux Back Track 5
Ubuntu Server	VSFTPD Server	LAMP Server (Linux, Apache, Mysql, PHP)
Fierce	Hydra	Sqlmap
Webmin 1.620	Webmin 1.620	Damn Vulnerable Web Application 1.0.7

For his part, Yumbo (2021) described the details of the evaluation of various autonomous instruction logic notations to improve integration in studies. Thus, Figure 3 evaluates a comparative table of classifier algorithms (Naive Bayes, Logistic Regression, K nearest neighbors, Support Vector Machines, Decision Trees and Random Forests) focused on information security, as seen in **Table 2**.

Table 2: Ranking of automated forecasting algorithms (Yumbo, 2021)

Classification Algorithms	Representation	Easy to explain	Fast to train	Easy and fast to implement	Easy to understand	Precise	Probabilistic Results
Logistic regression		✓	✓	✓	✓	✓	✓
K nearest neighbors		✓	✓	X	✓	X	✓
Support vector machines		X	X	X	X	✓	X
Naive bayes		✓	✓	✓	✓	✓	✓
Decision trees		✓	X	✓	X	✓	✓
Random forests		X	✓	X	X	X	X

According to Sangucho (2021) stated that it is important to apply the method used in this study to Windows servers because one of the main disadvantages of Windows is the constant occurrence of bugs or security flaws, and because the main benefit of the framework is to predict anomalies. That is, it shows that malware threats could affect Windows Server servers because they use vulnerability identifiers revealed by malicious code. Therefore, applying predictive models to organizations that implement certain types of Windows Server services in their technology infrastructure can help improve information security by suggesting different events to enable optimal results (Sangucho, 2021).

3.1. Algorithmic metrics procedure

For the test stage the characters were taken, to this group of data where each group embodies the data analysis of each algorithm pronounced within the research. Therefore, the predict method was applied to give an estimate for each class, the estimate will be in the range of 0 to 1, and the argmax method will be applied to return the class with the highest estimate. In this way, you only get 0 (bad) and 1 (good).

Table 3: K-Nearest Neighbor Ranking Report

Predicted label	Accuracy score	
	Bad	70
	Good	15
	Bad	Good
Actual label		

Table 3 shows the results of the Confusion Matrix for the k-nearest neighbors' algorithm; it correctly guesses 70 and 5 times for Bad and Good respectively. However, it also gets 15 false positives and 10 false negatives; that is, 15 times it predicted Bad when it was really Good, and 10 times it predicted Good when it was Bad.

Table 4: Confusion Matrix for the K nearest neighbor algorithm

	Accuracy	Completeness	F-value
Bad	0.823	0.87.5	0.85
Good	0.33	0.25	0.284
Accuracy			0.37

Therefore, we can calculate the accuracy and completeness of each class and thus the F1-scores for each label: The F1-score is the harmonic average of accuracy and completeness, where the F1-score reaches its best value at 1 (representing perfect accuracy and completeness) and its worst value at 0. It

is defined using the equation F1-score:

$$F\text{-value} = 2 \times (\text{Precision} \times \text{Exhaustiveness}) / (\text{Precision} + \text{Exhaustiveness})$$

In this way, you have the following formulation in order to find the precision, completeness, F-Value and accuracy as it is:

$$\text{Accuracy} = \text{TP} / (\text{TP} + \text{FP}) \quad \text{Completeness} = \text{TP} / (\text{TP} + \text{FN})$$

$$F\text{-value} = 2 \times (\text{Precision} \times \text{Exhaustiveness}) / (\text{Precision} + \text{Exhaustiveness})$$

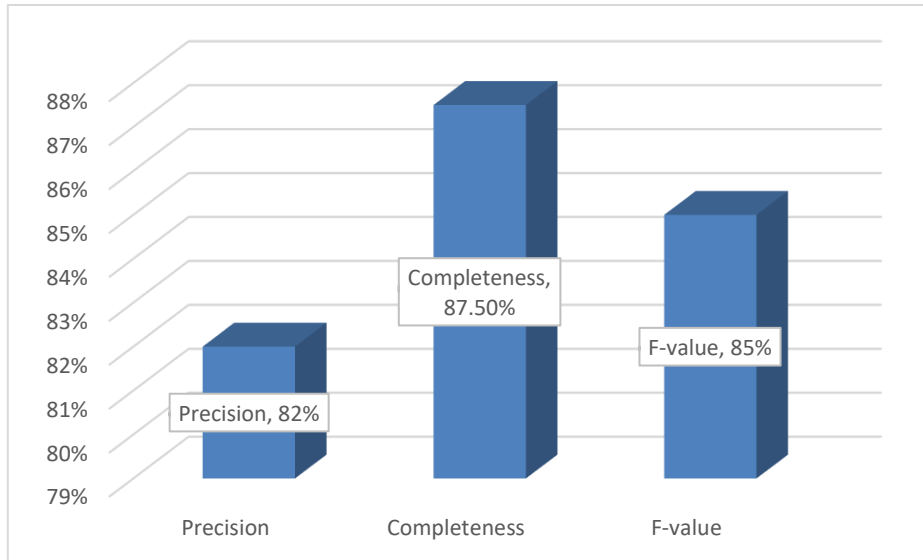


Fig. 2: Performance evaluation in the training stage and validation of negative accuracies for K nearest neighbors' algorithm.

Thus, Figure 2 determines the negative value equivalent to 0,

$$\text{Accuracy} = 70 / (70 + 15) = 0.823$$

$$\text{Completeness} = 70 / (70 + 10) = 0.875$$

$$F\text{-value} = 2 \times (0.823 \times 0.875) / (0.823 + 0.875) = 0.848$$

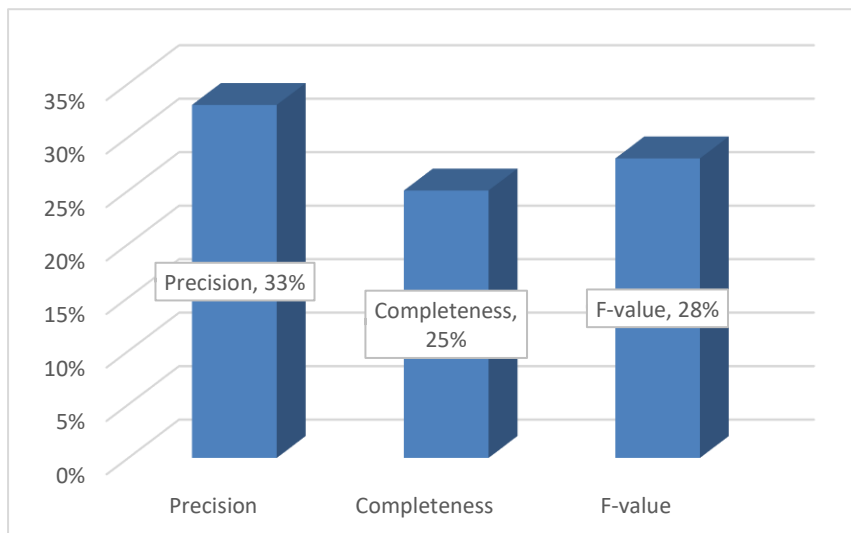


Fig. 3: Performance evaluation in the training stage and validation of positive accuracy metrics for K nearest neighbors' algorithm.

In this way, Figure 3 determines the positive value equivalent to 0,

Accuracy = $70 / (70+15) = 0.823$

Completeness = $70 / (70+10) = 0.875$

F-value = $2 \times (0.823 \times 0.875) / (0.823 + 0.875) = 0.848$

Subsequently, we have the final result of the accuracy of the K nearest neighbors' algorithm, of which the negative values are obtained as positive in the F value that will help to get the result of the accuracy.

$$(0.827 \times 25) + (0.546 \times 15) / 25 + 15 = 0.722$$

Table 5: Decision Tree Ranking Report

Predicted label	Accuracy score		
	Bad	24	1
	Good	9	6
	Bad	Good	
Actual label			

In Table 5, the results of the Confusion Matrix for decision trees are shown; it is correct 24 and 6 times for Bad and Good respectively. However, it also obtains 9 false positives and 1 false negative; that is, 9 times it predicted that it was Bad when it was really good, and 1 time it predicted that it was good when it was bad.

Table 6: Confusion Matrix for Decision Trees Algorithm

	Accuracy	Completeness	F-value
Bad	0.73	0.96	0.83
Good	0.86	0.4	0.55
Accuracy			0.72

Thus, in **Figure 4**, the negative value equivalent to 0 is determined,

Accuracy = $24 / (24+9) = 0.727$

Completeness = $24 / (24+1) = 0.960$

F-value = $2 \times (0.727 \times 0.960) / (0.727 + 0.960) = 0.827$

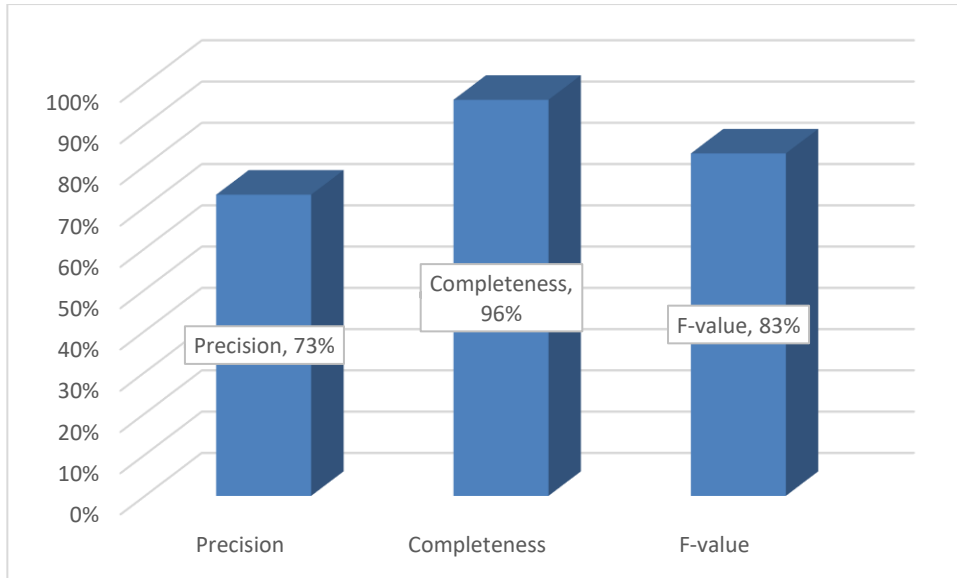


Fig. 4: Performance evaluation in the training and validation stage of the negative accuracy metrics for the Decision Trees algorithm.

Thus, in **Figure 5** the negative value equivalent to 0 is determined,

$$\text{Accuracy} = 6 / (6+1) = 0.857$$

$$\text{Completeness} = 6 / (6+15) = 0.40$$

$$\text{F-value} = 2 \times (0.857 \times 0.40) / (0.857 + 0.40) = 0.546$$

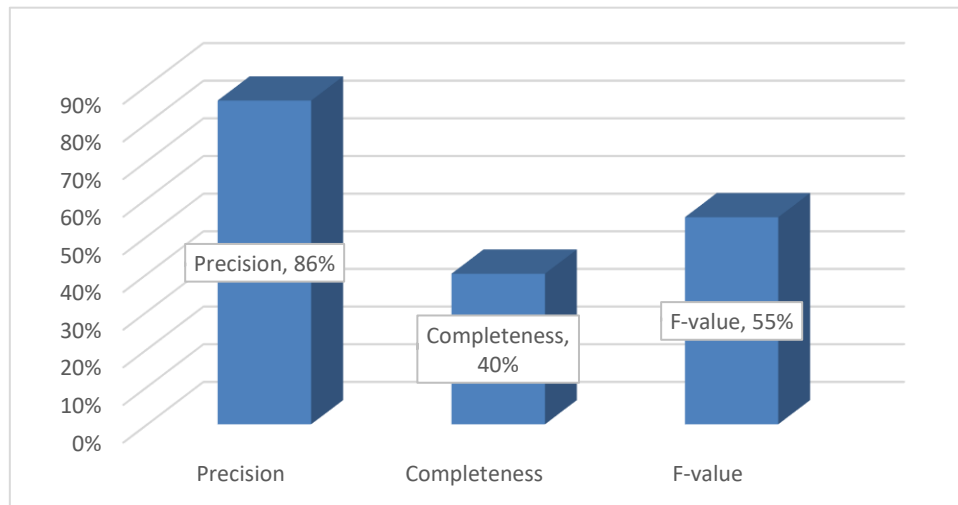


Fig. 5: Performance evaluation in the training and validation stage of the positive accuracy metrics for the Decision Trees algorithm.

On the other hand, we have the final result of the accuracy of the Decision Trees algorithm, from which the negative values have been obtained as positive in the F value that will help to obtain the result of the accuracy.

$$(0.848 \times 15) + (0.284 \times 80) / 15 + 80 = 0.37$$

Table 7: Naive Bayes Ranking Report

Predicted label	Accuracy score	
	Bad	24
	Good	2
	Bad	6
		18
	Bad	Good
	Actual label	

In Table 7, the results of the Confusion Matrix for Naive Bayes are visualized; it is correct 24 and 18 times for Bad and Good respectively. However, it also obtains 2 false positives and 6 false negatives; that is, 2 times it predicted that it was Bad when it was really Good, and 6 times it predicted that it was Good when it was Bad.

Table 8: Confusion Matrix for the Naive Bayes Algorithm

	Accuracy	Completeness	F-value
Bad	0.92	0.8	0.86
Good	0.75	0.9	0.82
Accuracy			0.84

Thus, in **Figure 6** the negative value equivalent to 0 is determined,

Accuracy = $24 / (24+2) = 0.923$

Completeness = $24 / (24+6) = 0.8$

F-value = $2 \times (0.923 \times 0.8) / (0.923 + 0.8) = 0.84$

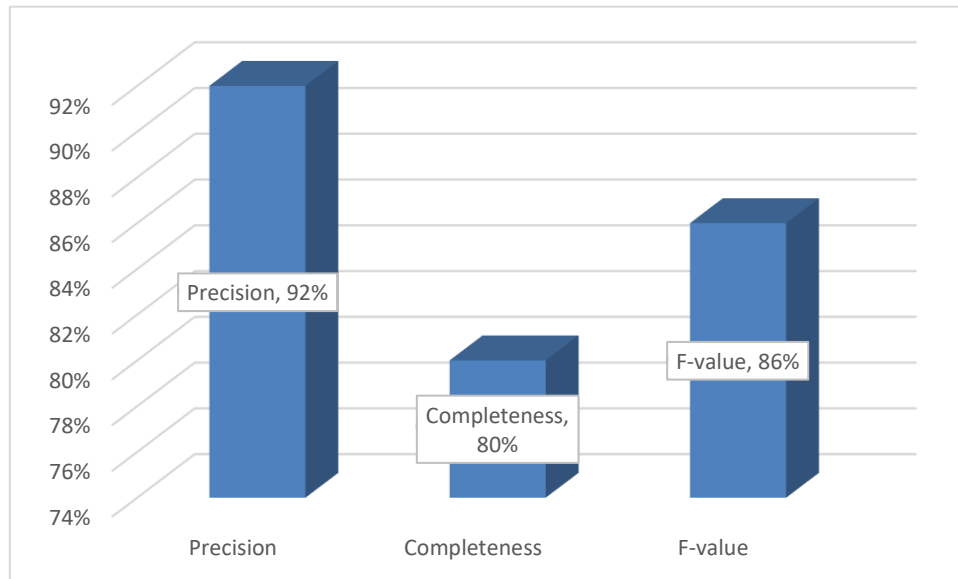


Fig. 6: Performance evaluation in the training and validation stage of the negative accuracy metrics for Naive Bayes algorithm.

Thus, in **Figure 7** the negative value equivalent to 0 is determined,

$$\text{Accuracy} = 18 / (18+6) = 0.75$$

$$\text{Completeness} = 18 / (18+2) = 0.9$$

$$\text{F-value} = 2 \times (0.75 \times 0.9) / (0.75 + 0.9) = 0.82$$

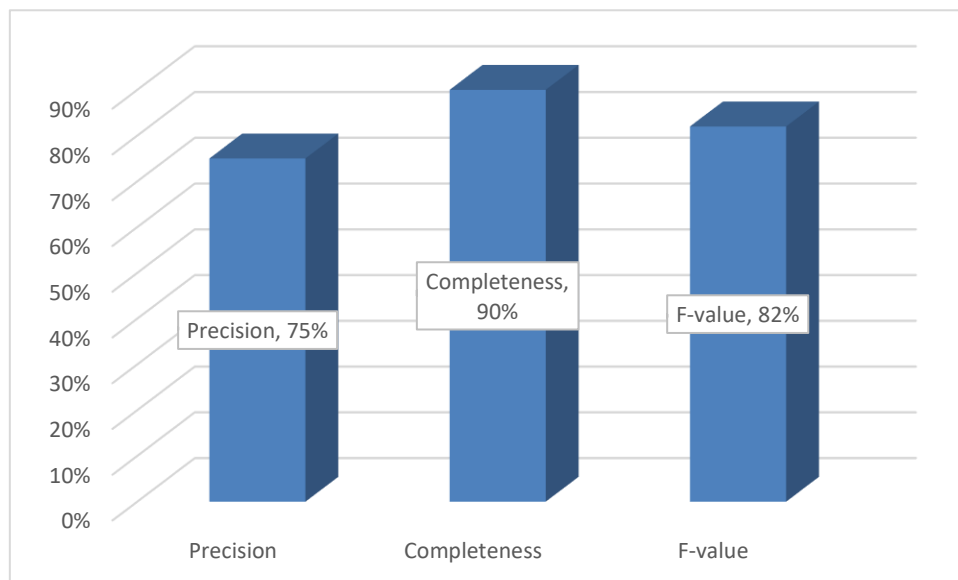


Fig. 7: Performance evaluation in the training and validation stage of the negative accuracy metrics for Naive Bayes algorithm.

On the other hand, we have the final result of the accuracy of the Naive Bayes algorithm, which has been obtained from the negative values as positive in the F value that will help to get the result of the accuracy.

$$(0.857 \times 30) + (0.82 \times 20) / 30 + 20 = 0.84$$

Table 9: Logistic Regression Ranking Report

Predicted label	Accuracy score	
	Bad	71
	Good	160
	Bad	Good
		Actual label

Table 9, which shows the results of the Confusion Matrix for Logistic Regression, correctly corrects 94 and 160 times for bad and good respectively. However, it also obtains 5 false positives and 71 false negatives; that is, 5 times it predicted that it was bad when it was really good, and 71 times it predicted that it was good when it was bad.

Table 10: Confusion Matrix for the Naive Bayes Algorithm

	Accuracy	Completeness	F-value
Bad	0.95	0.57	0.71
Good	0.69	0.97	0.81
Accuracy			0.76

Thus, in **Figure 8** the negative value equivalent to 0 is determined,

Accuracy = $94 / (94+5) = 0.949$

Completeness = $94 / (94+71) = 0.569$

$$\mathbf{F\text{-value}} = 2 \times (0.949 \times 0.569) / (0.949 + 0.569) = 0.84$$

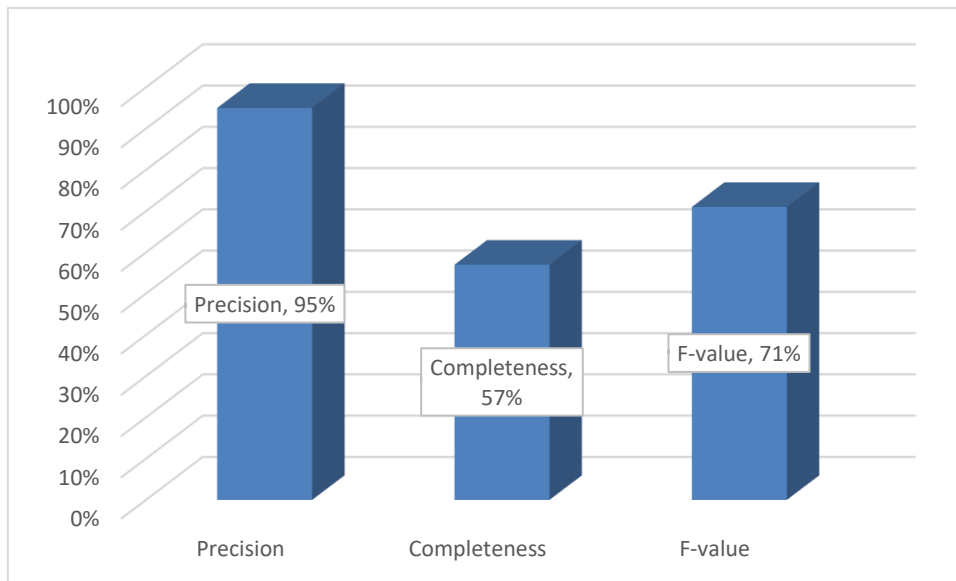


Fig. 8: Performance evaluation in the training and validation stage of the negative accuracy metrics for Logistic Regression algorithm.

Thus, in **Figure 9** the negative value equivalent to 0 is determined,

$$\mathbf{Accuracy} = 94 / (94 + 5) = 0.949$$

$$\mathbf{Completeness} = 94 / (94 + 71) = 0.569$$

$$\mathbf{F\text{-value}} = 2 \times (0.949 \times 0.569) / (0.949 + 0.569) = 0.84$$

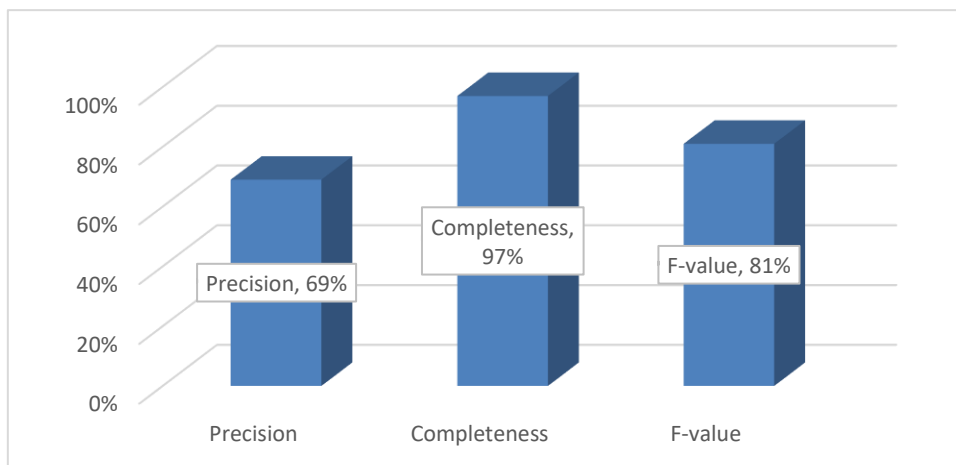


Fig. 9: Performance evaluation in the training and validation stage of the negative accuracy metrics for Logistic Regression algorithm.

Finally, we have the final result of the accuracy of the Naive Bayes algorithm, from which the negative values have been obtained as positive in the F value that will help to get the result of the accuracy.

$$(0.711 \times 165) + (0.811 \times 165) / 165 + 165 = 0.761$$

Table 10: Confusion Matrix for the Naive Bayes Algorithm

Algorithm	Class	Accuracy	Accuracy	Completeness	F-value
K nearest neighbors	Malo	0.37	0.82	0.88	0.85
	Good		0.33	0.25	0.28
Decision trees	Malo	0.72	0.73	0.96	0.83
	Good		0.86	0.4	0.55
Naive Bayes	Malo	0.84	0.92	0.8	0.86
	Good		0.75	0.9	0.82
Logistic Regression	Malo	0.76	0.95	0.57	0.71
	Good		0.69	0.97	0.81

When the confusion matrix is presented, the accuracy, precision, completeness and F-value metrics of each algorithm used for this study can be calculated. We can see the results in table 10, each algorithm has demonstrated a high performance, but Naive Bayes has obtained better results for each metric, followed by Logistic Regression, which by little margin to different results obtained by Decision Trees; in the case of K nearest neighbors results were obtained below Decision Trees, Logistic Regression and Naive Bayes. Therefore, we have the accuracy results for each algorithm evaluated within the research on cyber risk (Lee, 2022).

In summary, the algorithms are not very different, but it should be noted that the difference between algorithms is minimal, but they are essential for anomaly prediction, it makes no difference in the long run. Therefore, the applicability of any of the algorithms can be fully considered (Lee, 2022)

Sangucho (2021) states that the development of technology day by day goes beyond ideas with the incorporation of scientific advances. Just as every day new environmentally friendly technologies are created and all this technological advancement is accompanied by new vulnerabilities, nowadays it is not only about technology, it is also about the people behind it with the massive phishing mailing, which has taken place all over the country, with the theft of information, money, etc (Sangucho, 2021). Bonawitz et al. (2021) noted that security technologies support the structured enforcement of these expectations between parties, preventing participants from deviating even when they are malicious or compromised. In fact, the FL system can be considered a type of privacy protection technology in its own right, as it has a structure that prevents the server from accessing anything related to the client's data (Bonawitz et al., 2021).

We can state that the obtained results are related to the research of Cifre (2020) which manifests of an implementation of a security model based on vulnerability management of servers in private clouds, which defines a complete and effective process for vulnerability management, including security policy guidelines and detailed security process, will ensure the protection of the private cloud (Cifre, 2020).

4. Conclusions

It is concluded that as organizations grow, data becomes vulnerable to attack by cybercriminals who seek to harm and extort by means of privileged information. As a result, IT security focuses on all institutions. While there are several types of attacks based on vulnerabilities that affect information systems, techniques and tools have also been revealed to detect security problems and protect system information. This security system analysis facilitated certain entities and clients to develop strategies to address vulnerabilities.

By defining the theoretical foundations that make it possible to perform the test scenario, the necessary steps are established for performing the metric analysis of predictive algorithms focused on computer anomalies, which include various stages such as preliminary research, data collection, analysis and preparation of expert opinions; these analyses can determine the cause of the attack on the file server.

According to the research on different security consequences on the air in different servers and autonomous logical annotations, the evaluation criteria hosted by malicious programs are focused with shared keys, worms, data extraction and being able to steal the information of the entities, in the same way there are programs that can be very useful for a quick training, compression and ease of applying regulations that can opt for a solution to different malpractices developed. Similarly, we must consider that currently there are professionals who focus on these vulnerable details, it should be considered to have a specialized area that handles multidisciplinary in relation to computer security and monitor the processes of the entity.

These algorithms used in the labs help analyze and process data and improve the accuracy of each malware threat prediction. Security is a constantly evolving definition because it is a fundamental axis of national and international development. In this sense, cybersecurity has been consolidated as a broad term that faces the challenge of strategically balancing interrelated areas that require guidelines, spaces and priorities.

In relation to the test scenario, it was obtained that each algorithm has demonstrated high performance, but Naive Bayes has obtained better results for each metric, followed by Logistic Regression, which by little margin to different results obtained by Decision Trees; in the case of K nearest neighbor's results were obtained below the expected result (Portilla, 2022; Camacho, 2020). Therefore, the accuracy results for each algorithm evaluated within the research on cyber risk focused on servers (Portilla, 2022; Camacho, 2020). On the other hand, multiple recommendations will be specified based on the algorithm metrics, such as:

VPNs are recommended to manage PCs used remotely by users because they are not easy to vulnerate, in addition, to severely evaluate and validate the connection of has tools used when performing a scan for vulnerabilities (Ardila, 2019). Most tools are run by third parties and have a backdoor that activates DNS within the organization (Lazarte and Silva, 2022). On the other hand, a secondary option is to use virtual machines from Microsoft (Azure) or Amazon (Web Services) that function as a computer that can be manipulable at the user's disposal and is essential to perform computer testing or web development testing, configuration or installation of multiple systems and is an option for user activities (Meza and Imbachi, 2016).

On the other hand, constantly examine new threats posed by malware targeting Windows servers and generate alerting reports with the aim of reducing the consequences and impacts on the system. Indeed, it is necessary to validate the behavior of autonomous predictive notations of threats by malware through Naive Bayes and Logistic Regression for future implementation in organizations. Finally, it is necessary to implement the appropriate security layer to block hashes, URLs, emails and IP addresses related to malware.

References

Alvarenga, H. y Souza, L. (2020). El aumento de los ciberataques debido a la pandemia del covid-19. *Fatec*, 1-15. <http://ric.cps.sp.gov.br/handle/123456789/10422>

Álvarez, J. y Preciado, D. (2021). Evolución del fraude informático: una problemática en las organizaciones bancarias colombianas. *Tecnológico de Antioquia, Institución Universitaria*, 1-35. <https://dspace.tdea.edu.co/handle/tdea/2331>

Ameijeiras, D., Valdés, O. y González, H. (2021). Algoritmos de detección de anomalías con redes

profundas. Revisión para detección de fraudes bancarios. *Revista Cubana de Ciencias Informáticas*, 15(4), 244-264.

Analuisa, J. (2022). Análisis forense informático de un servidor de archivos institucional. [Pontificia Universidad Católica del Ecuador]. <https://repositorio.pucesa.edu.ec/handle/123456789/3480>

Ardila, N. (2019). Seguridad en las VPN´ S. Universidad Piloto de Colombia, 1-13.

Bonawitz, K., Kairouz, P., McMahan, B. y Ramage, D. (2021). *Federated Learning and Privacy*. *Queue*, 19(5), 114. <https://doi.org/10.1145/3494834.3500240>

Bugajski, M. (2019). Análisis de vulnerabilidades en redes corporativas. [Tesis para obtener el grado de ingeniería de las tecnologías de telecomunicaciones]. 1-186.

Caballero, I. (2020). Detección de actividad sospechosa en la red asociada con ataques cibernéticos en el ámbito ofimático. Universidad Pública de Navarra.

Camacho, D. (2020). Contribuciones en ciberseguridad y cibercrimen: 2021 AIDACyber. *Information Fusion*, 63, 1-33.

Camargo, L. (2020). Ciberseguridad y teletrabajo en tiempos de Covid-19. [Tesis para obtener el grado de maestría en periodismo]. Bogotá: Colombia.

Carpio, D. y Miralles, F. (2021). El impacto de redes de colaboración en la innovación tecnológica en empresas. *RETOS. Revista de Ciencias de la Administración y Economía*, 11(22), 315-331.

Chávez, K. y Moreno V. (2021). Diseño de un modelo de centro de operaciones de seguridad (SOC) para el control y monitoreo de normativas de seguridad informática, utilizando herramientas open source, para la Empresa Domobak en la Ciudad de Guayaquil. [Tesis para obtener el grado de título ingeniero en networking y telecomunicaciones]. 1-114.

Cifre, S. (2020). Modelo de seguridad para la gestión de vulnerabilidades de servidores en nubes privadas [Universidad Tecnológica Nacional Facultad Regional Santa Fe].

Díaz, M., Casas, R. y Giráldez, R. (2019). Análisis de las redes de colaboración en la innovación para el desarrollo. *Cooperativismo y Desarrollo*, 7(1), 5-25.

Escalante, O. (2021). Prototipo de sistema de seguridad de base de datos en organizaciones públicas para mitigar ataques cibernéticos en Latinoamérica. [Tesis para obtener el título de ingeniero de sistemas]. 1-21.

Espinoza, S. (2020). Responsabilidad civil objetiva de la actividad bancaria frente al fraude informático: phishing. *Ulaicit*, 1-23.

Franco, M. (2016). Ciberseguros, la mejor forma de transferir riesgos de ataques informáticos. *Universidad Piloto de Colombia*, 1-8.

Gamboa, J. (2020). Importancia de la seguridad informática y ciberseguridad en el mundo actual. *Universidad Piloto de Colombia*, 1-12.

Guaigua, C. (2021). Algoritmos de seguridad para mitigar riesgos de datos en la nube: un mapeo sistemático. [Tesis para obtener el grado de ingeniero de sistemas]. 1-12.

Lazarte, D. y Silva, G. (2022). Diseño de una red privada virtual (VPN) basada en software libre para la mejora de la seguridad de la información de la jurisdicción de la dirección de redes integradas de salud Lima Centro. [Tesis para obtener el título profesional de ingeniero de sistemas]. 1-145.

Lee, Y. (2022). A Study on Intermediate Code Generation for Security Weakness Analysis of Smart

Contract Chaincode. *Journal of Logistics, Informatics and Service Science*, 9(1), 53-67 pp. <https://doi.org/10.33168/LISS.2022.0105>

Martín, P. (2015). Inseguridad cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos. *Pre-bie3*, (4), 1-28.

Martínez, E. (2021). Delitos cibernéticos. *Transregiones*, (2), 93-104.

Meza, E. y Imbachi, D. (2016). Las ventajas de la utilización de Microsoft Azure en proyectos Open Source. *Algunas estrategias para mejorar la competitividad*, 6, 1-82.

Monterosso, E. (2019). Inteligencia artificial y riesgos cibernéticos: responsabilidades y aseguramiento. *Inteligencia artificial y riesgos cibernéticos*, 1-570.

Morales, J. (2022). Influencia del COVID 19 en el incremento de los Ciberataques a Nivel Mundial. *Universidad Piloto De Colombia*, 1-7.

Muñoz, P. (2021). Modelos de seguridad para prevenir riesgos de ataques Informáticos: Una revisión sistemática. [Tesis para obtener el grado de ingeniero de sistemas]. 1-14.

Nagli, L. (2020). Pandemia na pandemia: a escalada de ataques cibernéticos pós COVID-19. In *Congresso Transformação Digital 2020*.

Nunez, N. y Gatica, G. (2022). Applying Profit-driven Metrics in Predictive Models: A Case Study of the Optimization of Public Funds in Peru. *Journal of System and Management Sciences*, 12(2), 52-65. <https://doi.org/10.33168/JSMS.2022.0203>

Orozco, C. (2021). Estrategias algorítmicas orientadas a la ciberseguridad: Un mapeo sistemático [Tesis para obtener el título de ingeniero de sistemas]. 1-15.

Ovallos, J., Rico, D. y Medina, Y. (2020). Guía práctica para el análisis de vulnerabilidades de un entorno cliente-servidor GNU/Linux mediante una metodología de pentesting. *Iberian Journal of Information Systems and Technologies*, 5(29), 335-350.

Paredes, E. y Silva, E. (2021). Responsabilidad civil de los bancos frente al delito de fraude informático phishing en tiempos de Covid19 en Lima-2020. [Tesis para obtener el grado de título profesional de abogada]. 1-90.

Pérez, H. (2021). Seguro de riesgos cibernéticos: Enfoque y perspectivas en la nueva normalidad. *Revista de la Facultad de Derecho y Ciencias Sociales de la Universidad Católica de Córdoba*, 1(4).

Pin, L. y Pinargote, F. (2022). Análisis y simulación de COBALT STRIKE, metasploit y PUPYRAT para conocer las características o patrones de ataques. [Tesis para obtener el grado de título ingeniero en networking y telecomunicaciones]. 1-135.

Pinilla, C. (2021). Riesgos y vulnerabilidades en las bases de datos relacionales [Universidad nacional abierta y a distancia – UNAD].

Portilla, J. (2022). Desarrollo de un modelo clasificador de malware con algoritmos de aprendizaje automático. [Tesis para obtener el grado de título de ingeniero en telecomunicaciones]. 1-240.

Pozo, F. (2022). Nuevos delitos informáticos por impulso de la transformación digital por causa del Covid-19 en el Perú. [Tesis para obtener el grado de título profesional de abogado].

Ramírez, A. (2020). Análisis proactivo de amenazas de la seguridad informática y de la información para la infraestructura de servidores y red de la dirección de TIC de un GAD Municipal [Universidad Estatal Península de Santa Elena].

Rosas, W., Medina, F., y Mesa, J. (2020). Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas. *Revista ESPACIOS*, 41(07), 1-14.

Sangucho, A. (2021). Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del Cuerpo de Bomberos de Latacunga. *Revista Científica y Tecnológica VICTEC*, 2(3), 1-14.

Silva, D. (2020). Fraude cibernético: Cómo influye la falta de controles de seguridad y conocimiento en los ataques cibernéticos tanto en empresas privadas y gubernamentales como a nivel individual [Tesis para obtener el grado de maestría en sistema de información]. 1-73.

Terán, B., Dávila, G. y Castañón, I. (2019). Gestión de la tecnología e innovación: un Modelo de Redes Bayesianas. *Economía: teoría y práctica*, 1(50), 63-100.

Torres, H. (2022). Fraudes bancarios: algunos fraudes financieros y riesgos asociados. *Especialización en Gerencia Financiera*, 1-20.

Vera, A. (2020). Detección de anomalías en la red de la Empresa Newoffice utilizando algoritmos de aprendizaje automáticos [Tesis para obtener el grado de ingeniería en telecomunicaciones]. 1-100.

Villacis, V. (2018). Auditoría forense: metodología, herramientas y técnicas aplicadas en un siniestro informático de una empresa del sector comercial. [Tesis para obtener el grado de auditor en control de gestión]. 1-192.

Yumbo, L. (2021). Análisis de técnicas para la detección de amenazas de seguridad utilizando machine Learning aplicado a servidores Windows server 2016 [Tesis para obtener el grado de título de ingeniero en networking y telecomunicaciones]. 1-119.