Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

Cybercrime And Organized Crime in a Specialized Unit of the Public Prosecutor's Office in the Ancash Region - 2024

Dr. Rodríguez Silva Williams Marino

(orcid.org/0000-0002-0553-3485)

Dr. Medina Corcuera, Groberti Alfredo

(orcid.org/0000-0003-4035-157X)

Dra. Buleje Ayala, Lucía

(orcid.org/0000-0001-9764-220X)

ABSTRACT

This research aimed to determine the relationship between cybercrime and organized crime in a specialized unit of the public ministry of the Ancash - 2024 region. A methodology with a quantitative approach, of a basic type, non-correlational design and transversal scope was used in a sample of 35 prosecutors. To whom two questionnaires of closed questions with answers of the Likert scale type were administered; the first questionnaire of 20 items with reliability of $\alpha 1 = 0.935$; and the second questionnaire, of 20 items with reliability of $\alpha 2 = 0.922$. The results showed a high level of cybercrime with 48.6% and a medium perception of organized crime with 48.6%, presenting as a conclusion: a significant relationship was determined (Rho = 0.837; sig. = 0.000 < 0.05) between cybercrime and organized crime in a specialized unit of the public ministry of the Ancash region, referring that cybercrime and organized crime in the digital age are enhanced by interrelated factors that act as facilitators, these factors contribute to creating an environment of difficult regulation and surveillance.

Keywords: Cybercrime, Cybercrimes, Organized crime

INTRODUCTION

Latin America faces a complex cybersecurity scenario, where the increase in connectivity and the use of digital technologies has been accompanied by a significant increase in cybercrime, this situation poses serious challenges for the security of citizens, businesses and government institutions (Acosta et al., 2020). Many Latin American countries lack robust and updated legal frameworks that specifically address cybercrime, in addition, there is a lack of awareness of the importance of cybersecurity in both the public and private sectors, leaving organizations and individuals exposed to attacks, the most common crimes in the region include phishing, ransomware, identity theft and online fraud (Cancelado and Rodriguez, 2023). These crimes not only affect companies, but also have a direct impact on the daily lives of citizens, generating economic losses and affecting confidence in the digital environment, cyber insecurity has

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

significant economic repercussions, companies that suffer attacks can face financial losses, damage to their reputation and costs associated with data recovery, at the social level, distrust in the use of technologies can limit the development of the digital economy in the region (Santillán et al., 2022).

In the case of Peru, cyber crimes of different types such as credit card cloning, entity impersonation, extortion, etc., are evidenced through communication channels. Although the Peruvian law on cyber crimes is mainly found in the framework of the Penal Code and Law No. 30096, which establishes specific provisions for the prevention and punishment of computer crimes, this legislation seeks to protect the integrity of computer systems and the information handled in the digital environment (Pacheco, 2024). Criminal organizations have adopted cyber extortion techniques, using unauthorized access to computer systems of companies and individuals to obtain economic benefits, this type of crime has become increasingly common and sophisticated, taking advantage of the vulnerability of digital systems, cyber extortion is a clear example of how organized crime has adapted its methods to the digital age (Pino, 2023). This phenomenon not only represents a challenge for the security of companies and individuals, but also requires a coordinated and effective response from the authorities to combat it and protect society (Ruiz and Solís, 2024).

At the local level, the Public Prosecutor's Office has received several demands among them cyber crimes based on personnel who mainly use social networks to impersonate other personnel and get personal information of other personnel, which is used in organized crime such as extortion and violation of human rights, criminals use technological means to commit cyber crimes that violate the rights of people in different areas, the most common recorded are the impersonation used to extract information from minors about their families that are then used to commit crimes.

Under the above, the following question is posed: What is the relationship between cybercrime and organized crime in a specialized unit of the Public Prosecutor's Office in the Ancash region - 2024?

The justification that supports the study is based on the social aspect because the study of the cases presented to the Public Prosecutor's Office analyzes the factors involved and the consequences they generated, allowing to be interpreted and to obtain historical information that will allow the authorities to apply strategies that allow the strengthening of processes and optimize processes related to cybercrime and organized crime. Regarding the practical justification the development of the study involves a numerical analysis that leads to the interpretation of figures that allow the study of the levels of perception and correlation of the variables, regarding the methodology justification the execution of the study favors the knowledge through the adaptation of instruments that present theoretical sources and allow the

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

argument of the events of the variables and how it is reflected in the perception of the users. Finally, we have the theoretical justification, arguing that the development of the study obtains conclusions that respond to the objectives and broaden the knowledge of the variables, by means of literature review.

The general objective is to determine the relationship between cybercrime and organized crime in a specialized unit of the Public Prosecutor's Office of the Ancash Region - 2024. Then the specific objectives are described: To describe cybercrime in a specialized unit of the public ministry of the Ancash region - 2024. To describe organized crime in a specialized unit of the public ministry of the Ancash region - 2024.

Ponce (2024) published his article in the Scielo database with the purpose of analyzing computer crime in Ecuador. The study was considered descriptive because it analyzed the perception of computer crime, and cross-sectional because it was carried out at a single point in time. As a result, it was found that the country has all the judicial support to protect the integrity of citizens and punish people who violate the cyber privacy of the population. In addition, the most used modality is organized crime, generated by extortion and human trafficking.

Concepción (2022) has developed his article with the purpose of analyzing how cybersecurity is presented to achieve hybrid security in the United States. The methodology was of transversal scope as it was executed at a certain moment, then considered as non-experimental as it was observed without generating alteration of its behavior. As a result, it was described that the country has the necessary mechanisms to control computer crimes with sanctions depending on the severity presented, one of the most common factors presented is the impersonation to obtain information to violate the rights of the victims and cyber theft.

Muñoz et al. (2021) in Mexico presented their article in Scielo with the title comparative analysis of cyberbullying and self-efficacy in social networks. Regarding the methodology applied, it was qualitative, of cross-sectional scope, to be executed at a certain time, the technique used was the interview, where the opinions of the interviewees were collected, as results have been recorded that most of the aggrieved are minors, who are vulnerable to these forms of theft, for this it is necessary to implement the necessary measures for the state to protect the rights of victims and punish offenders.

Henríquez (2023) in Ecuador carried out his study disseminated in the Scielo database related to the analysis of the violation of human rights in the province of Huayas. The methodology was estimated of cross-sectional scope, presenting a single moment execution, of non-experimental design for carrying out observations without generating alteration of the events. As a result, it was found that children and adolescents are the most vulnerable people

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

and the most attacked by cybercriminals, because they are easier to manipulate and obtain information to violate their rights, in addition to the fact that impersonation is one of the most common ways to commit cybercrime.

Rodolfo et al. (2021) carried out their article in Chile, Mexico and Colombia with the purpose of analyzing computer crimes. Regarding the methodology applied was qualitative, cross-sectional in scope, to be executed at a certain time, the technique used was the interview, where the opinions of the interviewees were collected, as results have been recorded presentation of these crimes can vary in modality and technique, depending on the technology used and the social and legal context. In addition, the response to these crimes may involve collaboration between local and international authorities, due to the global nature of the Internet. To combat these crimes, it is essential to foster cybersecurity education, promote safe online practices, and establish appropriate laws that criminalize and sanction these criminal behaviors.

In the national context we have Anicama (2023), who has developed a study in Lima, in order to know the perception of computer crimes and the link it has with cybercrime. Regarding the methodology applied, it was qualitative, of cross-sectional scope, to be executed at a certain time, the technique used was the interview, where the opinions of the interviewees were collected, as results showed that young people are the main vulnerable to cybercrime because there have been reports of identity theft to extract information from their families and commit criminal acts, also cyber theft is another worrying factor in this issue by the constant attacks suffered by citizens to their credit cards with card cloning.

Condori (2020) in Lima has developed a study based on analyzing the legal implications of cyber fraud and the associated linkage to criminal protection. Referring to the methodology applied was qualitative, cross-sectional in scope, to be executed at a certain time, the technique used was the interview, where of I collect the opinions of the interviewees, as results have been recorded that Advances in computer technology are currently one of the most used tools in the daily activities of people due to its versatility and automation, allowing us to interact through online platforms. But unfortunately this platform has become a crime tool that affects both public and private property.

Castillo (2024) in Lima has executed his study based on analyzing the access to information through the modality of computer crime. Referring to the methodology applied was qualitative, cross-sectional in scope, to be executed at a certain time, the technique used was the interview, where of recopilo the opinions of the interviewees, as results it was discovered that confidential information the Department has access to information on organized crime investigations Public for criminal investigation purposes and follow the legal

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

mechanisms. Ask the examining magistrate to order the delivery Confidential intelligence and can continue investigating reaching the goal of truth.

Regarding the variable cybercrime, the theory refers to the set of principles and concepts that seek to explain and classify crimes committed through digital media, as technology advances, so do the forms of criminality, which makes it necessary to adapt traditional theories of crime to this new context (Mayer and Oliver, 2020). Cybercrime theory focuses on defining what constitutes a crime in the digital environment, this includes not only crimes that are committed exclusively online, such as hacking or phishing, but also those that have a digital component, such as financial fraud using digital platforms (Chanchí et al., 2022). The classification of these crimes is essential for their correct classification and punishment, as in traditional crime theory, the theory of cybercrime is based on the existence of certain elements: the action (criminal conduct), the result (damage caused), the typicality (adequacy to the norm) and culpability (intention of the perpetrator), however, in the digital environment, these elements can be more complex to identify and prove, which poses challenges for law enforcement (Saltos et al., 2021). Intentionality in cybercrime can be more difficult to establish due to the anonymity offered by the digital environment, which raises questions of culpability and responsibility of the perpetrator, especially in cases where automated tools are used or in a context of low supervision, cybercrime theory must also consider the impact of these crimes on society and the economy, cybercrimes not only affect direct victims, but can also have broader repercussions, such as loss of trust in digital platforms and the weakening of the digital economy (Alcalá and Meléndez, 2023).

In order to determine the dimensions of cybercrime, the following are used: First dimension cybercrime, are illegal activities that are committed through electronic means, especially on the Internet, this category encompasses a wide variety of criminal conduct, including, but not limited to, identity theft, online fraud, malware distribution, cyberstalking, unauthorized access to computer systems, cyber espionage and the dissemination of illegal content such as child pornography, cybercrime can have a significant impact on individuals, organizations and societies, affecting security, privacy and trust in digital technologies (Bazurto et al. , 2024).

Regarding the second dimension phishing is an online fraud technique that aims to trick people into revealing sensitive information such as passwords, credit card numbers and personal data, attackers use fake emails, text messages or websites pretending to be from legitimate institutions, such as banks or online services, to induce victims to provide their information, often, these communications contain elements of urgency or fear to motivate a quick response, and may include links to fraudulent web pages that appear authentic, phishing

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

is one of the most common forms of Internet scams and represents a serious risk to the security of personal information (Hernandez and Baluja, 2021).

In the third dimension, pharming is a malicious technique used to redirect Internet users from a legitimate website to a fake website, with the aim of stealing personal and confidential information. Unlike phishing, which usually involves direct deception through emails or messages, pharming alters the domain name resolution process, This can result in the user, when trying to access a legitimate web page, ending up in a fraudulent copy designed to look like the original, where they can be tricked into entering sensitive data, pharming represents a significant threat because it can affect multiple users and is more difficult to detect than other methods of deception (Dominguez and Vera, 2022).

Finally we have the ransomware dimension is a type of malware that encrypts the files of a user or an organization, preventing access to them until a ransom is paid, once the system has been infected, the attacker usually displays a message informing the victim about the encryption of their data and demands a payment, usually in cryptocurrencies, to provide the decryption key, this type of attack can affect personal computers, servers and entire networks, and can have devastating consequences for companies and organizations, both in terms of data loss and disruption of operations, ransomware is a serious cybersecurity problem and has increased in frequency and sophistication in recent years (Garcia and Herrero, 2021).

Regarding the second variable organized crime, the theory refers to the study and analysis of the structures, dynamics and activities of criminal groups that operate in a systematic and organized manner, these groups, which can involve from small local gangs to large transnational organizations, represent a significant challenge to public security and justice (Rincón, 2019). Organized crime is characterized by its hierarchical structure, where members have specific roles and work together to carry out illicit activities, these organizations are often involved in a variety of crimes, such as drug trafficking, extortion, money laundering and human trafficking, planning and coordination are essential to their operation, which distinguishes them from common crime (Guerra, 2024).

Regarding the first dimension, organic structure according to Law No. 30077, Art. 2.- refers to the internal model that criminal organizations adopt to operate in a coordinated and efficient manner according to the law, this structure implies a functional distribution of roles among members, where each member performs specific tasks to achieve the illicit objectives, this differentiates criminal organizations from common criminal groups since their operation resembles a company with hierarchies and division of labor (Res. Adm. No. 136-2012-CE_PJ allows authorities not only to pursue individual crimes, but also to dismantle all layers of a criminal organization, from the leaders to the smallest operators. It also highlights the

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

complexity and adaptability of these networks, as their structure allows them to operate clandestinely, coordinate actions in different regions and even infiltrate public institutions.

Social support is a dimension of organized crime for the authors Cullen, Wright and Chamlin (1999) social support in the context of organized crime refers to the network of interactions, relationships and legitimacy that these organizations build with communities or individuals who are directly or indirectly linked to their activities is not only a relationship of voluntary complicity, This support can be motivated by various reasons such as coercion, economic benefits, the perception of state absence, or even the construction of affective ties and trust between criminal leaders and individuals. They follow in their definition Lin (1996), Organized crime is a complex phenomenon that transcends the purely criminal sphere to enter into the social, economic and cultural dynamics of the communities where it operates among the multiple dimensions that shape its operation, social support occupies a fundamental place this dimension, understood as the ability of criminal organizations to gain the acceptance or tolerance of certain sectors of the population, strengthens its permanence and expansion becoming a key tool for its consolidation.... Dong and Krohn (2017) write that social support propositions imply that organized networks of human relationships help people cope with a set of needs and desires throughout the life course, which prevents criminal behavior, for Kort-Butler (2018) social support refers to the social resources one can rely on when facing life problems and sources of stress, with a reductive nuance, Robbers (2004) The social dimension of organized crime poses a particular challenge for states, as dismantling a criminal organization is not enough if its support in communities is maintained. It is essential to address the conditions that favor this social support, such as poverty, inequality and state absence. Thoits (1995) offers the following definition: emotional, informational, or practical assistance from significant others, such as family members, friends, or co-workers, clarifying that assistance may be actually received from others or simply perceived to be available for when it is needed. Woo et al., (2016) and colleagues offer a definition for the correctional setting that is basically service provision.

For García and López (2019). The logistical dimension of organized crime, is something that uses day by day in many areas and crime has it as a support tool to carry out their criminal actions, employs the electronic device, the management of economic resources, influences and knowledge of technological tools among other strengths allows criminal organizations to be strengthened. For Stock INTERPOL. (2017). Organized crime is a complex phenomenon that transcends the purely criminal sphere to enter the social, economic and cultural dynamics of the communities where it operates among the multiple dimensions that shape its operation, social support occupies a fundamental place this dimension, understood as the ability of criminal organizations to gain the acceptance or tolerance of certain sectors of the population, strengthens its permanence and expansion, becoming a key tool for its consolidation.

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

According to Interpol (2017), social support in the context of organized crime refers to the network of interactions, relationships and legitimacy that these organizations build with communities or individuals who are directly or indirectly linked to their activities it is not only a relationship of voluntary complicity, This support can be motivated by various reasons, such as coercion, economic benefits, the perception of the absence of the state, or even the construction of affective ties and trust between criminal leaders and individuals.

As a general hypothesis it has been established: There is a significant relationship between cybercrime and organized crime in a specialized unit of the Public Prosecutor's Office in the Ancash region - 2024.

METHODOLOGY

According to the characteristics reflected in the study it is considered as basic, in this regard Hernandez and Mendoza (2018), define it to basic research, also known as fundamental or pure research, refers to scientific inquiry that seeks to expand knowledge without an immediate practical objective, this type of research is essential for the development of new theories, concepts and technologies that can have a significant impact on various disciplines.

Arias and Covinos (2021) refer that it is a research method based on the collection and analysis of numerical data to identify patterns, relationships and trends. This approach is fundamental in various disciplines, from the social sciences to the natural sciences, and offers a series of advantages that make it indispensable in scientific research.

According to the design is characterized as non-experimental, Carrasco (2019), mentions that it is a research design in which the researcher observes and analyzes phenomena without manipulating variables or assigning treatments to the study subjects, in this type of design, it seeks to understand relationships, patterns and trends in existing data or in natural situations, It is often used in descriptive, correlational and exploratory studies, where the objective is to identify associations between variables without establishing causality. This approach is particularly useful in the social sciences and humanities, where the manipulation of variables may be unethical or impractical.

The correlational level is a type of research design that focuses on examining the relationship between two or more variables without manipulating them, in this approach, it seeks to determine whether there is an association or correlation between variables, as well as the direction and strength of that relationship, correlational studies use statistical methods to analyze data and calculate correlation coefficients, This level of research is useful for identifying patterns and trends, but does not allow establishing causal relationships, since no variable is controlled or manipulated. It is commonly used in social sciences, psychology and

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

education to explore links between factors such as attitudes, behaviors and results (Carhuancho et al. , 2019).

Cross-sectional scope, also known as cross-sectional study, is a research design that is characterized by the collection of data at a single point in time, this approach allows researchers to examine and analyze different variables and their relationship in a specific population at a specific time, without conducting follow-ups over time, cross-sectional studies are useful to identify patterns, trends and prevalence of phenomena, trends and prevalence of phenomena, as well as to explore associations between variables, however, due to their snapshot nature, they do not allow establishing causal relationships or observing changes over time, this type of design is common in research in areas such as public health, sociology and psychology, where the aim is to obtain a snapshot of the situation of a particular group or population (Cohen and Gomez, 2019).

In the context of research, the population refers to the total set of individuals, elements or units that share specific characteristics and that are the object of study, the population can be broad or restricted, depending on the focus of the research, for example, a population can include all the students of a university, all the inhabitants of a city or all the products of a production line (Hadi et al., 2023). In the case of the research, the population is made up of 35 prosecutors on average in the Ancash Public Prosecutor's Office.

The sample is a representative subset of the population that is selected to participate in a study, the choice of an adequate sample is crucial, since it allows researchers to make inferences about the population as a whole without the need to study all its members, the sample should be large and diverse enough to reflect the characteristics of the population, and can be selected randomly or non-randomly (Jimenez, 2020). In the case of the study, the sample is made up of all the subjects analyzed in the population.

Sampling is the process by which a sample is selected from the population, there are different sampling methods, which can be classified into two main categories: probability sampling and non-probability sampling, probability sampling implies that each member of the population has a known and non-zero probability of being selected, which allows generalizing the results to the population, on the other hand, non-probability sampling does not guarantee that all members of the population have the same opportunity to be selected, which may limit the generalizability of the findings (Montalván et al. , 2019).

A survey is a method of data collection used to obtain information about the opinions, attitudes, behaviors or characteristics of a specific group of people. Surveys can be administered in a variety of ways, including face-to-face interviews, telephone surveys, online surveys or paper questionnaires.

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

A questionnaire is a data collection instrument consisting of a set of questions designed to elicit specific information from respondents, questionnaires may include closed-ended questions (with predefined response options) and open-ended questions (allowing free responses), questionnaires are often used as part of a survey, and their design is crucial to ensure the clarity, relevance and validity of the questions, a good questionnaire facilitates the collection of accurate and useful data for subsequent analysis.

Validity refers to the degree to which a measurement instrument, such as a questionnaire or a test, actually measures what it is intended to measure. It is a fundamental concept in research, since it ensures that the results obtained are relevant and applicable to the phenomenon under study, and there are different types of validity, including content validity (which evaluates whether the content of the instrument is representative of the construct being measured), criterion validity (which compares the results of the instrument with an external standard) and construct validity (which examines whether the instrument actually measures the theoretical concept it is intended to evaluate).

Reliability refers to the consistency and stability of a measurement instrument over time and under different conditions; a reliable instrument produces similar results when applied repeatedly under the same circumstances. Reliability can be assessed by different methods, such as correlation coefficient, internal consistency (e.g., using Cronbach's alpha coefficient), and temporal stability (through testing and retesting). A high level of reliability is essential to ensure that research results are accurate and reproducible.

Descriptive statistics is a branch of statistics that is responsible for summarizing, organizing and presenting in a clear and understandable way the data collected in a study, it uses numerical measures, such as mean, median, mode, variance and standard deviation, as well as graphs and tables, to describe the characteristics of a data set, the objective of descriptive statistics is to provide an overview of the data, facilitating the identification of patterns, trends and anomalies without making inferences about a larger population.

Inferential statistics is the branch of statistics that deals with making generalizations and predictions about a population from a representative sample, it uses statistical methods and techniques to estimate population parameters, test hypotheses and calculate confidence intervals, through inferential statistics, researchers can make decisions and draw conclusions based on sample data, thus allowing inferring characteristics and behaviors of the population as a whole, this approach is essential in scientific research, as it allows validating theories and making predictions based on empirical data.

The ethical aspects of research refer to the principles and norms that guide the conduct of researchers in the design, execution and dissemination of their studies. These aspects are

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

fundamental to ensure integrity, fairness and respect for participants and the community at large. The main ethical issues include:

Informed Consent: Researchers should obtain voluntary consent from participants, ensuring that they understand the nature of the study, the risks and benefits, as well as their right to withdraw at any time. Confidentiality: It is essential to protect the privacy of participants, ensuring that personal information and data collected are treated confidentially and used only for the purposes of the study. Minimization of Harm: Researchers should strive to avoid causing physical, psychological, or emotional harm to participants, as well as to the community at large. This involves careful assessment of the risks associated with the research.

Fairness: The selection of participants should be equitable, avoiding exploitation of vulnerable groups and ensuring that the benefits and burdens of research are distributed fairly. Scientific Integrity: Researchers should conduct their work with honesty and transparency, avoiding plagiarism, falsification of data and manipulation of results.

RESULTS

Descriptive statistics.

Table 1.

Frequency levels of the cybercrime variable and its dimensions

Dimensions and variable	Under		Medium		High		Total	
	fi	%	fi	%	fi	%	fi	%
D1: Cybercrime	5	14.3%	14	40.0%	16	45.7%	35	100.0%
D2: Phishing	8	22.9%	13	37.1%	14	40.0%	35	100.0%
D3: Pharming	4	11.4%	17	48.6%	14	40.0%	35	100.0%
D4: Ransomware	4	11.4%	18	51.4%	13	37.1%	35	100.0%
V1: Cybercrime	4	11.4%	14	40.0%	17	48.6%	35	100.0%

According to what was established by the perception of the subjects intervened for the completion of the instruments, the following is mentioned: According to the dimension Cybercrime evidencing the following information, the level that characterizes is the high with 45.7%, from there the medium level is presented with 40.0% and the low level is presented with 14.3%. The argument recorded for the phishing dimension has been characterized by the high level with 40.0%, then the medium level is presented with 37.1% and the low level is estimated with 22.9%. Correspondingly, for the pharming dimension, the highest score was reached at the medium level with 48.6%, followed by the high level with 40.0% and the low level with 11.4%. Concerning the ransomware

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

dimension it is characterized at the medium level with 51.4%, the high level with 37.1% and the low level with 11.4%. Finally, the analysis recorded for the cybercrime variable is presented with a score of 48.6% at the high level, then the medium level is presented with 40.0% and the low level with 11.4%.

Table 2.

Frequency levels of the organized crime variable and its dimensions

Dimensions and variable	Under		Medium		High		Total	
	fi	%	fi	%	fi	%	fi	%
D1: Organic structure	3	8.6%	20	57.1%	12	34.3%	35	100.0%
D2: Social support	4	11.4%	13	37.1%	18	51.4%	35	100.0%
D3: Logistics	5	14.3%	15	42.9%	15	42.9%	35	100.0%
D4: International character	5	14.7%	20	58.8%	9	26.5%	34	100.0%
V2: Racketeering	3	8.6%	17	48.6%	15	42.9%	35	100.0%

According to what was established by the perception of the subjects intervened for the filling out of the instruments, the following is mentioned: According to the dimension organic structure evidencing the following information, the level that characterizes is the medium level with 57.1%, from there the high level is presented with 34.3% and the low level is presented with 8.6%. The argument recorded for the social support dimension was characterized by the high level with 51.4%, then the medium level is presented with 37.1% and the low level is estimated with 11.4%. For the logistics dimension, the highest score was reached at the medium level with 42.9%, followed by the high level with 42.9% and the low level with 14.3%. Regarding the international dimension, it is characterized at the medium level with 58.8%, the high level with 26.5% and the low level with 14.7%. Finally, the analysis recorded for the organized crime variable shows a score of 48.6% at the high level, then the medium level with 42.9% and the low level with 8.6%.

Inferential analysis

As a means of arguing for the most appropriate method for the study, a normality test was developed to reveal the estimates that characterize the study.

Table 3.

Normality analysis

	Shapiro-Wilk		
	Statistician	gl	Sig.

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

Cybercrime	,932	35	,033
Organized crime	,942	35	,063

The method used to determine normality was Shapiro-Wilk, this is relevant when the sample does not exceed 50 and given that the characteristics of the study comply with the aforementioned, a significance was determined that on average is located below 0.05, with Spearman's Rho being the most appropriate method for the study.

Table 4.

Correlation between cybercrime and organized crime

			Cybercrime	Racketeering
Rho de Spearman	Cybercrime	Correlation coefficient	1,000	,837**
		Sig. (bilateral)	.	,000
		N	35	35
	Racketeering	Correlation coefficient	,837**	1,000
		Sig. (bilateral)	,000	.
		N	35	35

Based on the calculations obtained in the study, an Rho=0. 837, which estimates that there is a positive and moderate relationship between cybercrime and organized crime, indicating that cybercrime and organized crime in the digital era are enhanced by interrelated factors that act as facilitators, these factors contribute to create an environment of difficult regulation and surveillance, in which criminals can operate with great effectiveness and low risk of being caught, facing this problem requires a multidisciplinary approach and international cooperation to develop more robust regulations and a security infrastructure to mitigate existing vulnerabilities.

Next, the hypothesis evaluation was developed, for which it was essential to analyze the significance value reached, where a value of 0.000 was obtained, which when contrasted with the 0.05 is affirmed to be lower and thus proceeded to reject Ho.

DISCUSSION

After the argumentation developed the discussion is established for it is taken as a first instance to the general objective established as analyzing the relationship between cybercrime and organized crime in a specialized unit of the public ministry of the Ancash region - 2024, from the calculations obtained in the study has determined a Rho=0. 837 which estimates that there is a positive and moderate relationship between cybercrime and organized crime, stating that cybercrime and organized crime in the digital era are enhanced by interrelated factors that

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

act as facilitators, these factors contribute to create an environment of difficult regulation and surveillance, in which criminals can operate with great effectiveness and low risk of being caught, facing this problem requires a multidisciplinary approach and international cooperation to develop more robust regulations and a security infrastructure to mitigate existing vulnerabilities. Next, the hypothesis evaluation was developed, for which it was essential to analyze the significance value reached, where a value of 0.000 was obtained, which when contrasted with the 0.05 is affirmed to be lower and thus proceeded to reject Ho.

This is in agreement with what is expressed by Anicama (2023), who has developed a study in Lima, in order to know the perception of cybercrime and the link it has with cybercrime. Regarding the methodology applied, it was qualitative, of cross-sectional scope, to be executed at a certain time, the technique used was the interview, where the opinions of the interviewees were collected, as results showed that young people are the main vulnerable to computer crimes because there have been reports of identity theft to extract information from their families and commit criminal acts, also cyber theft is another worrying factor in this issue by the constant attacks suffered by citizens to their credit cards with card cloning.

The definition of cybercrime is a crucial issue in the field of cybersecurity and legislation, given the increasing use of digital technologies in everyday life, as interactions and transactions move to the digital environment, it is critical to establish a clear understanding of what constitutes a cybercrime (Jimenez, 2024). A cybercrime is commonly defined as any criminal activity that is carried out through digital means or that targets computer systems, networks or devices, this includes a wide range of behaviors, from unauthorized access to systems to online fraud and malware distribution (Avila and Rincon, 2023).

Regarding the specific objective of describing cybercrime in a specialized unit of the Public Prosecutor's Office in the Ancash region - 2024, according to the perception of the subjects interviewed for the completion of the instruments, the following is mentioned: According to the dimension Cybercrime evidencing the following information, the level that characterizes is the high with 45.7%, from there the medium level is presented with 40.0% and the low level is presented with 14.3%. The argument recorded for the phishing dimension has been characterized by the high level with 40.0%, then the medium level is presented with 37.1% and the low level is estimated with 22.9%. For the pharming dimension, the highest score was reached at the medium level with 48.6%, followed by the high level with 40.0% and the low level with 11.4%. Concerning the ransomware dimension it is characterized at the medium level with 51.4%, the high level with 37.1% and the low level with 11.4%. Finally, the analysis recorded for the cybercrime variable is presented with a score of 48.6% at the high level, then the medium level is presented with 40.0% and the low level with 11.4%.

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

Cybercrime regulations are insufficient or non-existent in several countries, allowing cybercriminals to exploit legal loopholes; companies and governments do not always implement appropriate cybersecurity protocols, leaving them vulnerable to attacks; the lack of international cooperation on cyber legislation issues allows criminals to find refuge in permissive jurisdictions or those with little regulation on cybercrime. What was described agrees with what was expressed by Condori (2020) in Lima, who developed a study based on analyzing how the legal implications of cyber fraud and the associated link to criminal protection are presented. Regarding the methodology applied, it was qualitative, The technique used was the interview, where the opinions of the interviewees were gathered. The results show that advances in information technology are currently one of the most used tools in people's daily activities due to its versatility and automation, allowing us to interact through online platforms. But unfortunately this platform has become a crime tool that affects both public and private property.

The transnational nature of cybercrime complicates its definition and prosecution, a crime may be perpetrated in one country, affect victims in another and be investigated by authorities in a third, highlighting the need for a definition that is recognized and applied internationally, the evolution of technology requires that legal definitions of cybercrime are constantly updated to include new forms of digital crime, this is essential to ensure that laws are effective and can adequately address emerging threats (Arapa et al., 2023).

With respect to the specific objective of describing organized crime in a specialized unit of the Public Prosecutor's Office in the Ancash region - 2024, according to the perception of the subjects interviewed for the completion of the instruments, the following is mentioned: According to the dimension organic structure evidencing the following information, the level that characterizes is the medium with 57.1%, from there the high level is presented with 34.3% and the low level is presented with 8.6%. The argument recorded for the social support dimension was characterized by the high level with 51.4%, then the medium level is presented with 37.1% and the low level is estimated with 11.4%. For the logistics dimension, the highest score was reached at the medium level with 42.9%, followed by the high level with 42.9% and the low level with 14.3%. Regarding the international dimension, it is characterized at the medium level with 58.8%, the high level with 26.5% and the low level with 14.7%. Finally, the analysis recorded for the organized crime variable shows a score of 48.6% at the high level, then the medium level with 42.9% and the low level with 8.6%.

Technology has facilitated the commission of crimes through advanced tools that allow both unauthorized access to systems and the development of strategies to hide digital footprints, malware, social engineering and ransomware are widely used tools in cybercrime, and are constantly evolving to circumvent security defenses, this allows organized crime to expand its

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

activities to the digital environment, optimizing the traffic of stolen data, extortion, and fraud. The above is in agreement with what Castillo (2024) in Lima has expressed in his study based on analyzing the access to information through the modality of computer crime. Referring to the methodology applied was qualitative, cross-sectional in scope, to be executed at a certain time, the technique used was the interview, where of recopilo the opinions of the interviewees, as results it was discovered that confidential information the Department has access to information on organized crime investigations Public for criminal investigation purposes and follow the legal mechanisms. Ask the examining magistrate to order the delivery Confidential intelligence and can continue investigating reaching the goal of truth. Organized crime is characterized by its hierarchical structure, where members have specific roles and work together to carry out illicit activities, these organizations are often involved in a variety of crimes, such as drug trafficking, extortion, money laundering and human trafficking, planning and coordination are essential to their operation, which distinguishes them from common crime (Guerra, 2024).

COCLUSIONS

A significant relationship (Rho= 0.837; sig.=0.000<0.05) was determined between cybercrime and organized crime in a specialized unit of the public ministry of the Ancash region, referring that cybercrime and organized crime in the digital era are enhanced by interrelated factors that act as facilitators, these factors contribute to create an environment of difficult regulation and surveillance.

Cybercrime in a specialized unit of the public ministry of the Ancash region, is presented with a score of 48.6% at the high level, then the medium level is presented with 40.0% and the low level with 11.4%, the evaluation of the dimensions is located at the medium level.

Organized crime in a specialized unit of the Public Prosecutor's Office in the Ancash region is presented with a score of 48.6% at the high level, then the medium level is presented with 42.9% and the low level with 8.6%, the evaluation of the dimensions is located at the medium level.

REFERENCES

1. Acosta et al. (2020). *Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios.* Revista Venezolana de Gerencia, vol. 25, núm. 89. https://www.redalyc.org/journal/290/29062641023/29062641023.pdf
2. Alcalá, M. y Meléndez, M. (2023). Computer crimes in Mexico. Recognition in the criminal laws of the Mexican entities. *PAAKAT: revista de tecnología y Sociedad. 13 (24).* https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072023000100005

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

3. Anicama, Y. (2023). *Delitos informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022.* [Tesis de posgrado; Universidad César Vallejo]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/122811/Anicama_AYA-SD.pdf?sequence=1&isAllowed=y
4. Arapa et al. (2023). Causes and consequences of the increase in computer crimes in the city of puno 2023. *Redalyc.* https://doi.org/10.47712/rd.2024.v9i1.262
5. Arias, J. y Covinos, M. (2021). *Diseño y metodología de la investigación.* ISBN: 978-612-48444-2-3. https://repositorio.concytec.gob.pe/handle/20.500.12390/2260
6. Ávila, F. y Rincón, P. (2023). Inclusion of prevention and handle of cybercrime in police education training. *Revista Educación. 47 (2).* http://dx.doi.org/10.15517/revedu.v47i2.53905
7. Bazurto et al. (2024). La ciberdelincuencia y la protección de datos personales. Sinergia Académica, 7(Especial 5), 594-612. https://doi.org/10.51736/sa.v7iEspecial 5.389
8. Cancelado, H. y Rodríguez, V. (2023). *The impact of transnational organized crime on the contemporary international system.* Revista Científica General José María Córdova. 21. (43). http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1900-65862023000300628
9. Carhuancho, I., Nolazco, F., Sicheri, L., Guerrero, M., & Casana, k. (2019). *Metodología de la investigación holistica. Guayaquil: Editorial UIDE. Repositorio Digital UIDE* https://repositorio.uide.edu.ec/handle/37000/3893
10. Carrasco, S. (2019). *Metodología de la investigación cientifica.* Lima: Editorial San Marcos.
11. Castillo, G. (2024). *Acceso a la información clasificada en las investigaciones penales por crimen organizado, Lima 2023-2024.* [Tesis de pos grado; Universidad Cesar Vallejo]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/147097/Castillo_AG-SD.pdf?sequence=1&isAllowed=y
12. Chanchí et al. (2022). *Characterization of cybercrime in the department of Cundinamarca during the first half of 2021 through exploratory analysis and machine learning.* Ingeniería y competitividad. 25 (1). https://doi.org/10.25100/iyc.v25i1.11760
13. Cohen, N. y Gómez, G. (2019). Metodología de la investigación, ¿para qué?: la producción de los datos y los diseños. ISBN 978-987-723-190-8. Editorial Teseo. http://biblioteca.clacso.edu.ar/clacso/se/20190823024606/Metodologia_para_que.pdf
14. Concepción, M. (2022). How important is cybersecurity to achieving water security?. *56 (1). Revista de Ciencias Ambientales.* http://dx.doi.org/10.15359/rca.56/1.15
15. Condori, R. (2020). *Implicancias Jurídicas del Fraude Informático y la Protección Penal del Delito Contra el Patrimonio Distrito*

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

Fiscal de Lima Norte 2020. [Tesis de pos grado; Universidad Cesar Vallejo]. https://repositorio.ucv.edu.pe/handle/20.500.12692/63158

16. Cullen, F. T., Wright, J. P. y Chamlin, M. B., (199) «Social support and social reform: A progressive crime control agenda», *Crime and Delinquency*, 45, 2, 1999
17. Domínguez, R. y Vera, R. (2022). Spatial analysis of cybercrime to e-commerce: considerations for political agenda in Tamaulipas. *Podium. 41 (1).* http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2588-09692022000100021
18. Dong, B. y Krohn, M. D., (2017) «The protective effects of family support on the relationship between official intervention and general delinquency across the life course», *Journal of Developmental and Life-Course Criminology*, 3, 2017.
19. García, J. y Herrero, L. (2021). Cyberdefense in the military healthcare information systems. Sanidad Militar. *76 (3).* https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1887-85712020000300140
20. García, J. y López, A. (2019). El crimen organizado en América Latina: una perspectiva multidimensional. Revista de Estudios Criminológicos, 23(2), 45- 62.
21. Guerra, E. (2024). Criminal Organizations. Applying a General Systems Theory Framework. *Estudios sociológicos. 41 (123).* https://doi.org/10.24201/es.2023v41n123.2292
22. Hadi, M., Martel, C., Huayta, F., Rojas, R. y Arias, J. (2023). *Metodología de la investigación: Guía para el proyecto de tesis.* ISBN: 978-612-5069-63-4 https://editorial.inudi.edu.pe/index.php/editorialinudi/catalog/view/82/124/149
23. Henríquez, R. (2023). Delitos informáticos: Vulneración de los derechos humanos en niñas, niños y adolescentes en la provincia de Guayas, *2014-2023. Derechos humanos y justicia juvenil. 4 (1).* https://revistas.uasb.edu.ec/index.php/andares/article/view/4446
24. Hernández, A. y Baluja, W. (2021). Main mechanisms for dealing with phishing in data networks. *Revista Cubana de Ciencias Informáticas. 15 (4).* http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992021000500413
25. Hernández. R. y Mendoza, C. (2018). *Metodología de la investigación- rutas cuantitativa-cualitativa-mixta.* ISBN 1456260960. Editor McGraw-Hill Interamericana. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/SampieriLasRutas.pdf
26. Jiménez, I. (2020). El triángulo lógico. Una ecuación didáctica emergente para aprender metodología de la investigación. Universidad de La Sabana. https://web.p.ebscohost.com/ehost/detail/detail?vid=0&sid=7be0c0b1-aae9-471f-ba3a-

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

42032829f293%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#db=e000xww&AN=2659814

27. Jimenez, L. (2024). The Current State of Cybercrime in Peru and German Law. *Boletín mexicano de derecho comparado. 56 (167).* https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332023000200197&lng=es&nrm=iso&tlng=es
28. Kort-Butler, L. A., (2018) *Social support theory*», en The Encyclopedia of juvenile delinquency and Justice (C. J. Schreck ed.), New York, Wiley-Blackwell, 2018.
29. Lin, N., (1986) *«Conceptualizing social support», in social support, life events, and depression* (N. Lin et al. eds.), Orlando, Academic Press, 1986.
30. Mayer, L. y Oliver, G. (2020). The crime of cyber fraud: Definition and delimitation. *Revista chilena de derecho y tecnología. 9 (1).* https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000100151
31. Montalván, J., Soria, C., Hopkins, A., Ascue, R. y Ajito, E. (2019). *Guía de investigación.* ISBN: 978-612-4439-09-4. Primera edición digital. https://cdn02.pucp.education/investigacion/2016/06/12214732/guia-de-investigacion-en-diseno.pdf
32. Muñoz et al. (2021). Comparison of cyberbullying and self-efficacy in social networks: Mexico City and the State of Mexico. *Escritos de Psicología (Internet). 14 (1).* https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1989-38092021000100002
33. Pacheco, W. (2024). La *Evolución de la Criminalidad Organizada a Nivel Nacional y la Seguridad Ciudadana.* 5 (1). https://recide.caen.edu.pe/index.php/recide/article/view/142
34. Pino, E. (2023). *International Organized Crime and its Impact on the Ecuador-Peru Frontier.* Podium. Podium no.44 Samborondón. 44 (1). http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2588-09692023000200133
35. Ponce, M. (2024). Computer Crimes: The Ecuador Case. *Revista San Gregorio. 1 (58).* https://doi.org/10.36097/rsan.v1i58.2667
36. Rincón, D. (2019). Organized crime and corruption: absence of penal liability in the "corruption for fear. *Revista Criminalidad. 61 (1).* http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082019000100127
37. Robbers, M. L. P., (2004) «Revisiting the moderating effect of social support on strain: A gendered test», *Sociological Inquiry*, 74, 2004.
38. Rodolfo et al. (2021). Cyber crimes in Chile, México and Colombia. A comparative law study. *Un estudio de Derecho Comparado. Ius Comitiãlis, [S.l.], 4 (8), p. 252-276, ISSN 2594-1356.* https://iuscomitialis.uaemex.mx/article/view/17320

Power System Technology
ISSN:1000-3673

Received: 16-09-2024 Revised: 05-10-2024 Accepted: 22-11-2024

39. Ruiz, P. y Solís, J. (2024). *Fraude informático en la modalidad de phishing en* Lima. https://revistaescpograpnp.com/ojs/index.php/1/article/view/166
40. Saltos et al. (2021). Conceptual analysis of computer crime in Ecuador. *Conrado. 17 (78).* http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442021000100343
41. Santillán et al. (2022). *Drugs, trafficking and organized crime as a trigger for violent acts in Ecuador's prisons.* Revista Universidad y Sociedad. 14v (3). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202022000300478
42. Stock J. INTERPOL. (2017). *Informe anual 2016*. https://www.interpol.int/content/download/4996/file/Annual%20Report%202016-ES.pdf?inLanguage=esl-ES
43. Thoits, P. A., (1995) «Stress, coping, and social support processes: Where are we? What next?», *Journal of Health and Social Behavior*, número. extra, 1995.
44. Woo, Y., Stohr, M. K., Hemmens, C., Lutze, F., Hamilton, Z. y Yoon, O.-K. (2016) «An empirical test of the social support paradigm on male inmate society», *International Journal of Comparative and Applied Criminal Justice*, 40, 2, 2016.