Presentation date: February, 2022
Date of acceptance: May, 2022
Publication date: August, 2022

PRINCIPALES TIPOS DE DELITOS INFORMÁTICOS EXISTENTES EN ECUADOR

Mesías Elías Machado Maliza[1]
E-mail: ur.mesiasmachado@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-5815-1093
Cristina Mercedes Rosero Moran[2]
E-mail: ut.cristinarm00@uniandes.edu.ec
ORCID: https://orcid.org/0000-0001-9618-3574
Alex Javier Peñafiel Palacios[3]
E-mail: ub.alexpenafiel@uniandes.edu.ec
ORCID: https://orcid.org/0000-0003-0352-1365
[1] Universidad Regional Autónoma de Los Andes. Riobamba. Ecuador
[2] Universidad Regional Autónoma de Los Andes. Tulcán. Ecuador
[3] Universidad Regional Autónoma de Los Andes. Babahoyo. Ecuador

Suggested citation (APA, 7th ed.)

Machado Maliza, M. E., Rosero Moran, C. M., & Peñafiel Palacios, A. J., (2022). Main types of computer crimes existing in Ecuador. *Revista Universidad y Sociedad*, 14(S4), 611-619.

ABSTRACT

The introduction and use of Information and Communication Technologies (ICT) have meant a vertiginous leap in scientific-technical development on a global scale, they have become an indispensable element in all facets of society. Without a doubt, the use of the Internet makes life easier for users, but those benefits become dangerous when unscrupulous people silently infiltrate to damage not only technical equipment but also the finances of individuals, companies, and governments. The objective of the investigation is to determine the main types of computer crimes existing in Ecuador, as well as the possible solutions to avoid them. Different research techniques and methods were studied, such as synthetic analytical, inductive deductive, logical historical, as well as the descriptive method, interviews, and surveys in the same way that tools such as descriptive surveys and referential research were used. To fulfill the proposed objective, the AHP Saaty and Vikor multicriteria methods were used, where the crimes with the highest probability of occurring in the country and the best techniques to combat them were obtained as conclusions.

Keywords: computer crimes, internet, experts, AHP Saaty, Vikor

RESUMEN

La introducción y uso de las Tecnologías de la Información y la Comunicación (TIC) han supuesto un salto vertiginoso en el desarrollo científico-técnico a escala mundial, se han convertido en un elemento indispensable en todas las facetas de la sociedad. Sin duda, el uso de Internet facilita la vida de los usuarios, pero esos beneficios se vuelven peligrosos cuando personas sin escrúpulos se infiltran silenciosamente para dañar no sólo los equipos técnicos sino también las finanzas de particulares, empresas y gobiernos. El objetivo de la investigación es determinar los principales tipos de delitos informáticos existentes en Ecuador, así como las posibles soluciones para evitarlos. Se estudiaron diferentes técnicas y métodos de investigación, como el analítico sintético, el deductivo inductivo, el histórico lógico, así como el método descriptivo, las entrevistas y las encuestas, del mismo modo que se utilizaron herramientas como las encuestas descriptivas y la investigación referencial. Para cumplir con el objetivo propuesto se utilizaron los métodos multicriterio AHP Saaty y Vikor, donde se obtuvieron como conclusiones los delitos con mayor probabilidad de ocurrencia en el país y las mejores técnicas para combatirlos.

Palabras clave: delitos informáticos, internet, expertos, AHP Saaty, Vikor

INTRODUCTION

Currently, Information and Communication Technologies (ICTs) are present in most activities of daily life, to a greater or lesser extent all areas of knowledge use information systems to perform tasks that at other times were done manually. For this purpose, it is incredible the possibility of accessing so much information, so diverse and so public, at the hand of any user, in the history of humanity.

Today, there is a wide variety of content in this regard, such as wikis, virtual libraries, chat, email, videoconferences, electronic signatures, forums, blogs, and robotics, among others, which facilitate any type of mass interaction, without taking into account considering age, gender or economic level, who rely on these contents to entertain themselves, socialize, search for information from the comfort of home, office or any environment where there is an internet connection (Acosta et al, 2020). Technological advances in the creation, processing, storage, and transmission of data have opened new doors to various forms of cybercrime (Núñez & Carhuancho, 2020).

Computer crimes can be defined as the set of behaviors that generates a criminal offense and that must be treated legally since it is intended to damage third parties, causing different injuries and, in some cases, loss of legal assets. It is necessary to clarify that this type of crime occurs in cyberspace. Internationally there are different designations for the terminology computer crimes, such as electronic crimes, cybercrime, computer-related crimes, and computer crimes, among others. (López, 2020). The term most used by the authors in the doctrine of computer criminal law is computer crime.

The fraudulent manipulation of computers for profit, the destruction of programs or data, and the improper access and use of information that may affect the sphere of privacy, are some of the procedures related to the electronic processing of data through the which it is possible to obtain great economic benefits or cause significant material or moral damage (Saltos et al, 2021). But not only is the amount of damage caused in this way often infinitely higher than that which is usual in traditional crime, but the chances that it will not be discovered are also much higher (Zambrano & Ordoñez, 2016).

Computer crimes cover a wide variety of modalities as mentioned on the Interpol website and listed below:

- Attacks against computer systems and data
- Identity theft
- Distribution of images of sexual assaults against minors (child pornography)
- Internet scams
- Intrusion into online financial services
- Spread of viruses
- Botnets (networks of infected computers controlled by remote users)
- Phishing (fraudulent acquisition of sensitive personal information)

However, they are not the only ones, there are also risks related to the use of social networks and access to all kinds of information such as:

- Access to inappropriate material (illicit, violent, pornographic, etc.)
- Addiction - procrastination (distractions for users)
- Socialization problems
- Identity theft
- Harassment (loss of privacy)
- Sexting (management of erotic content)
- Cyberbullying (harassment between minors by various means: mobile, internet, video games, etc.)
- Cyberrooming (method used by pedophiles to contact children and adolescents in social networks or chat rooms)

The Computer Crime Treaty is defined as an international instrument that covers crimes committed through the use of the Internet and computer networks. Its objective is to apply a criminal policy that seeks to protect society against cybercrime, through the incorporation of specialized legislation and international cooperation. It covers issues related to procedural law, such as the expeditious preservation of stored data, partial disclosure of traffic data, the production order, the search and seizure of computer data, the real-time collection of traffic data, and the interception of content data. It encompasses a set of provisions and thematic areas that include the following:

- Crimes against the confidentiality, availability, and integrity of data and computer systems.
- Crimes related to the use of computers include those corresponding to forgery and fraud.
- Crimes related to content specifically pornography.
- Crimes related to the violation of copyright and associated rights.
- Secondary responsibilities and sanctions for criminal cooperation, and corporate responsibility in the commission of crimes.

In general, according to (Miro, 2021), the main characteristics of computer crimes are:

- White-collar criminogenic conduct.
- They are occupational actions, insofar as they are often carried out when the subject is working.
- They are actions of opportunity, in that an opportunity created or highly intensified in the world of functions and organizations of the technological and economic system is taken advantage of.
- They cause serious economic losses since they almost always produce "profits" of more than five figures for those who carry them out.
- They offer facilities of time and space since in thousandths of a second and without a necessary physical presence they can be consummated.
- There are many cases and few complaints, and all of this is due to the same lack of regulation by the Law.
- They are very sophisticated and relatively common in the military field.
- They present great difficulties for their verification, due to their very technical nature.
- They are mostly reckless and not necessarily committed with intent.
- They offer facilities for their commission to minors.
- They tend to proliferate more and more, so they require urgent regulation.
- For the time being, they continue to be illicit acts that manifestly go unpunished before the law.

From the foregoing, it can be seen that those who commit this type of illicit act are people with knowledge of computers and cybernetics, who are in strategic places or with ease to access sensitive information, such as credit or government institutions. In most cases, they damage the property of the victim, who, due to the lack of law applicable to the specific case, is not reported, leaving these types of antisocial behavior unpunished.

The behaviors or actions that the United Nations considers to be computer crimes are the following:

- Fraud committed through computer manipulation: this type of computer fraud, also known as data theft, represents the most common computer crime.
- The manipulation of programs; this crime consists of modifying existing programs in the computer system or inserting new programs that have specialized knowledge in computer programming.
- Output data manipulation; It is done by setting a target for the operation of the computer system, the most common example being ATM fraud by forging instructions to the computer in the data acquisition phase.
- Fraud carried out by computer manipulation of computing processes.
- Computer counterfeits: when data from documents stored in computerized form is altered.
- As instruments; computers can also be used to falsify business documents
- Computer sabotage; is the act of unauthorized deletion, suppression, or modification of computer functions or data to interfere with the normal operation of the system.
- The virus is a series of programmatic keys that can attach to legitimate programs and spread to other computer programs.
- The worms; are analogous to a virus to infiltrate legitimate data processing programs or modify or destroy data, but it is different from a virus because they cannot regenerate themselves.
- The logical or chronological Bomb; requires specialized knowledge since it needs the programming of the destruction or modification of data at a given time in the future.
- Unauthorized access to services or computer systems; is for various reasons from simple curiosity, as in the case of many hackers, to sabotage or computer espionage.
- Hackers or Hackers; this access is often made from an external location, located in the telecommunications network.
- Unauthorized reproduction of legally protected computer programs; brings a substantial economic loss for the legitimate owners.

Computer crimes are already typified in the legal framework of Ecuador, in the Law of Electronic Commerce, Data Messages and Electronic Signatures, and the Comprehensive Organic Criminal Code (Ecuador. Asamblea Nacional, 2014). Cybercrime in Ecuador has evolved as the number of users on the network increases. As a result, computer crimes have increased dramatically over the last five years. According to what was stated by (Peralta & Aguilar, 2021) in the country, 83% of the population has access to the Internet, allowing them to be connected to the information that is in cyberspace, which is a gateway for criminals, thus increasing the risk to security. According to the complaints made in the Prosecutor's Offices of Ecuador, 8,421 cases of cybercrime were registered at the national level in 2017; in 2018 these figures increased to 9,571 and in 2019 to 10,279, noting a constant trend that continues to grow.

A crime cannot be punished if it is not duly defined in the legal framework; that is to say, all behavior that threatens the harmony and tranquility of the social conglomerate must be normalized, since it is not possible to sanction it through analogies. For this reason, the creation of punitive criminal types of new illicit crimes as a result of technological progress such as those that are developed through the internet is required, these are cyberbullying, cyberattacks, auctions, and illegal sales on the internet, use of robot or zombie networks, etc.

The objective of the present work is to analyze the elements that make up the computer crimes typified in the Comprehensive Criminal Organic Code of Ecuador, as well as the elements to take into account to avoid being a victim of their application. For this, two multi-criteria decision methods (MCDM) were used: Saaty's Analytic Hierarchy Process (AHP) and Vikor due to the versatility in decision-making and expert criteria.

MATERIALS AND METHODS

Next, the theoretical and empirical methods used throughout the present investigation that is presented to fulfill the outlined objectives are described.

- Analytical-Synthetic Method: the analytical method allowed the decomposition of the whole in specific aspects to understand and understand the structure; making it easy to observe to better understand the components. In this context, this method implies synthesis, that is, the union of dispersed elements to form a total component.
- Inductive-Deductive Method: with its application it is possible to know the reality of the problem under investigation, starting from the particular to the general and from the general to the particular of the problem.
- Historical-Logical Method: allows knowing the source of the problem and its progress to compare it with the actuality of the problem.
- Descriptive Method: with its application, it is possible to objectively describe the current reality in which the problem develops and thus demonstrate the existing problem of this tax regulation that affects this vulnerable group and society.
- Interviews: will be applied to the sample made up of selected experts. Structured interviews were prepared aimed at obtaining information on the real problem and issuing possible solutions, to obtain valid conclusions and support the results.
- Surveys: they are developed and applied to the experts who will intervene in decision-making.

The Analytic Hierarchy Process (AHP Saaty) was proposed by Thomas Saaty in 1980 (Saaty, 2001). This method can be applied to situations involving technical, economic, political, social, and cultural factors. In other words, it aims to be a scientific tool to address those aspects that are difficult to quantify, but that sometimes requires a unit of measurement. (Abdel-Basset & Mohamed, 2021). The basic hierarchy is made up of general goals or objectives, criteria, and alternatives. The hierarchy is constructed in such a way that the elements are of the same order of magnitude and can be related to some of the next levels (Cisnero et al, 2020).

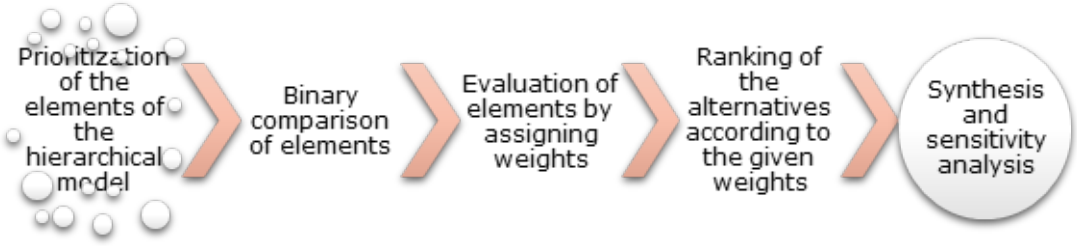

Figura 1. Saaty's AHP methodology. Source: Adapted from (Abdel-Basset & Mohamed, 2021).

For step 1, the following evaluation scale proposed by the author of the method will be used:

Table 1: Saaty Evaluation Scale (Verbal Judgment Rate). 2021)

Scale	
9 Extremely Most Preferred	3 Moderately more preferred
7 Very Powerfully Most Preferred	1 Equally Preferred
5 Powerfully Most Preferred	

Source: (Abdel-Basset & Mohamed,

An algorithm for calculating this is presented below (this must be applied to all criteria):

For each line of the pairwise comparison matrix, determine a weighted sum based on the sum of the product of each cell by the priority of each corresponding alternative or criterion

- For each line, divide its weighted sum by the priority of its corresponding alternative or criterion
- Determine the mean λ_{max} of the result of the previous stage
- Calculate the consistency index (CI) for each alternative or criterion

$$CI = \frac{\lambda_{max} - m}{m-1} \quad (1)$$

- where m is the number of alternatives
- Determine the Random Index (RI) from table 2
- Determine the consistency quotient index (the ratio of the consistency index to the random index)

Table 2: Random index for the calculation of the consistency coefficient.

Number of alternatives for decision n	Random Index	Number of alternatives for decision n	Random Index
3	0.58	7	1.32
4	0.9	8	1.41
5	1.12	10	1.49
6	1.24		

Source: (Abdel-Basset & Mohamed, 2021)

The VIKOR method (VIseKriterijumska Optimizacija I Kompromiso Resenje) was proposed by Serafín Opricovic in 1990. Determine the ranking of the alternatives using the aggregation function Q, which represents the "closeness to the ideal", calculated from the aggregation of the maximum group utility function S and the individual regret function R (Opricovic & Tzeng, 2007; Abdel-Baset, et al., 2019; Paronyan, et al, 2020).

Steps:

- Definition of the Decision Matrix with the respective weights (wi) of each criterion.
- Linear normalization of the decision matrix.

$$f_{ij}(x) = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \quad i = 1, \dots, m \; ; j = 1, \dots, n \quad (2)$$

Determination of the best () and the worst () values in the evaluations of each criterion (i=1,2,...,n) and alternatives (j=1,2...,j) defined as follows: $f^* f^-$

$$f_j^* = Max_i f_{ij} \, , f_j^- = Min_i f_{ij} \; ; \; j = 1,2, \dots, n \quad (3)$$

$$f_j^* = Min_i f_{ij} \, , f_j^- = Max_i f_{ij} \; ; \; j = 1,2, \dots, n \quad (4)$$

$$f^* = \{f_1^*, f_2^*, f_3^*, \dots, f_n^*\} \quad (5)$$

$$f^- = \{f_1^-, f_2^-, f_3^-, \dots, f_n^-\} \quad (6)$$

Calculation of the measures S, R, and Q for each alternative.

$$S_j = \sum_{i=1}^{n} w_i \left(\frac{f_j^* - f_{ij}}{f_j^* - f_i^-} \right) \quad (7)$$

$$R_i = Max_j \left[w_j \frac{(f_j^* - f_{ij})}{(f_j^* - f_j^-)} \right] \quad (8)$$

Each of the obtained vectors generates a ranking by organizing their values from lowest to highest and with them, the Q values are calculated:

$$S^* = min_j S_j \qquad S^- = max_j S_j \quad (9)$$

$$R^* = min_j R_j \qquad R^- = max_j R_j \quad (10)$$

Verification of the acceptable advantage condition and the acceptable stability condition in decision making

Definition of the compromise solution(s).

$$Q_j = v \frac{S_j - S^*}{S^- - S^*} + (1 - v) \frac{R_j - R^*}{R^- - R^*} \quad (11)$$

DISCUSSION AND RESULTS

A survey was designed for the experts to determine the criteria on which to evaluate the different types of computer crimes present in Ecuador. Next, the resulting table is presented with the weights after having carried out the binary comparison matrix of the AHP Saaty with the following criteria:

A. Crimes of threats and defamation
B. Network security violations
C. Child pornography
D. Seizure of computer data
E. Computer fraud
F. Inappropriate use of devices
G. Copyright infringement
H. Systems interference

Table 3: Normalized matrix with the resulting weights from the binary comparison matrix of the AHP Saaty. Source: own elaboration

Criteria	A	B	C	D	E	F	G	H
A	0.33	0.35	0.41	0.22	0.36	0.24	0.17	0.27
B	0.33	0.35	0.41	0.37	0.26	0.33	0.23	0.27
C	0.07	0.07	0.08	0.22	0.16	0.14	0.17	0.12
D	0.11	0.07	0.03	0.07	0.05	0.14	0.10	0.12
E	0.05	0.07	0.03	0.07	0.05	0.05	0.03	0.12
F	0.07	0.05	0.03	0.02	0.05	0.05	0.23	0.04
G	0.07	0.05	0.02	0.02	0.05	0.01	0.03	0.01
H	0.05	0.05	0.03	0.02	0.02	0.05	0.03	0.04

Table 4: Consistency analysis. Source: own elaboration

Criteria	Weight	W x Weight	Approx. Eigenvalues
Crimes of threats and defamation	**0.29**	2.65	9.078247407
Network security violations	**0.32**	2.90	9.147096099
child pornography	**0.13**	1.15	9.040958686
Seizure of computer data	**0.09**	0.75	8.732429806
computer fraud	**0.06**	0.50	8.564794635
Inappropriate use of devices	**0.07**	0.56	8.303486000
copyright infringement	**0.03**	0.29	9.219025670
systems interference	**0.04**	0.31	8.779721349

When performing the consistency analysis, according to the proposed method, an eigenvalue of 8.85822, CI=0.12, and RC= -0.09 was obtained, which allows us to affirm that the criteria of the experts are consistent. It can be concluded that of the criteria on the main computer crimes present in Ecuador, those that are carried out most frequently are network security violations, among them we have theft from bank accounts, identity theft, and acts of corruption.

Another of the most common crimes is the crime of threats and defamation where cybercriminals hide behind social networks to threaten and defame innocent people and the other with greater continuity is the crime of child pornography

in which the pedophile impersonates a child to win the child's friendship and in this way seek the minor to send him or her nudes or acts of a sexual nature.

An analysis of the main alternatives that are counted to avoid being victims of these computer crimes was carried out, for the understanding of the same the Vikor Method was used, executing separate consultations to the groups of experts. Having 6 alternatives and 8 criteria to analyze. The results of this analysis are shown in Tables 5, 6, 7, and 8 below.

Table 5: Weights and characteristics of the criteria. Source: own elaboration

Nr.	Decision criteria	Decision Magnitude	Weights (AHP)
A	Crimes of threats and defamation	+	0.29
B	Network security violations	+	0.32
C	child pornography	+	0.13
D	Seizure of computer data	+	0.09
E	computer fraud	+	0.06
F	Inappropriate use of devices	+	0.07
G	copyright infringement	+	0.03
H	systems interference	+	0.04

Table 6: Normalized decision matrix. Source: own elaboration

Alternatives/Criteria	A	B.	C	D	E	F	G	H
Avoid giving confidential information online	0.324	0.385	0.542	0.463	0.452	0.278	0.315	0.456
Do not install free programs if you do not know the manufacturer	0.445	0.346	0.25	0.294	0.503	0.51	0.539	0.319
Avoid connecting to public networks if you don't know the owner	0.283	0.577	0.459	0.379	0.302	0.417	0.494	0.41
Avoid having access codes to social networks, bank accounts, etc. on the devices.	0.485	0.385	0.459	0.337	0.352	0.417	0.36	0.502
Create hard-to-guess passwords by combining numbers, uppercase letters, lowercase letters, and special characters	0.526	0.423	0.334	0.547	0.452	0.51	0.27	0.319
Use security applications on devices such as anti-virus and/or firewall	0.324	0.269	0.334	0.379	0.352	0.232	0.405	0.41

Table 7: Determination of the values S, R, and Q. Source: Own elaboration

Alternatives	S	R	Q
Avoid giving confidential information online	0.495	0.104	0.099
Do not install free programs if you do not know the manufacturer	0.51	0.125	0.624
Avoid connecting to public networks if you don't know the owner	0.494	0.125	0.598
Avoid having access codes to social networks, bank accounts, etc. on the devices.	0.433	0.104	0.039
Create hard-to-guess passwords by combining numbers, uppercase letters, lowercase letters, and special characters	0.458	0.125	0.5
Use security applications on devices such as antivirus and/or firewall	0.746	0.125	1

Table 8: Ranking of the alternatives. Source: own elaboration

Alternatives	Rank in S	Rank in R	Rank in Q
Avoid giving confidential information online	4	2	2
Do not install free programs if you do not know the manufacturer	5	3	5
Avoid connecting to public networks if you don't know the owner	3	3	4
Avoid having access codes to social networks, bank accounts, etc. on the devices.	1	1	1
Create hard-to-guess passwords by combining numbers, uppercase letters, lowercase letters, and special characters	2	3	3
Use security applications on devices such as antivirus and/or firewall	6	3	6

According to the exercise; the alternative with the minimum value of Q will be selected as the best alternative if both conditions are met. In this case, alternative 4 was selected as the best alternative to protect against computer crime, which translates into Avoid having access codes to social networks, bank accounts, etc. on the devices. It is followed by alternative 1: Avoid giving confidential information over the internet and the third is alternative 5: Create difficult-to-guess passwords, combining numbers, uppercase and lowercase letters, and special characters.

CONCLUSIONS

As information technology and communications take center stage in the lives of human beings, they are more exposed to new risks and possible attacks on their privacy. It is essential to maintain a safe communication environment for all users, the main challenge for the governments of the countries is the implementation of a regulatory framework that allows curbing the exponential growth of computer crimes in recent years.

The Law in Ecuador is generalized on the subject of computer crimes, they are typified in the Law of Electronic Commerce, Data Messages, and Electronic Signatures and the Comprehensive Organic Criminal Code (COIP) although the sanctioning framework does not cover all possible crimes taking into account that every day cybercriminals use new methods to carry out their acts and that they are not typified in any law, which is why it needs to be reformed and specified according to each type of crime and be constantly updated through changes in society and technology to provide security to Internet users.

Surveys were designed for experts to determine the criteria on which to evaluate the different types of computer crimes present in Ecuador and the main alternatives that are available to avoid being victims of these computer crimes.

An analysis was carried out using the AHP Saaty method to determine the computer crimes that most affect the country, concluding that those that are carried out most frequently are network security violations, threats and defamation crimes, and child pornography crimes.

An analysis was carried out using the VIKOR method to determine the main alternatives that are available to avoid being victims of these computer crimes. In this case, they were selected as the best alternatives to protect against computer crime to avoid having network access codes on the devices. social accounts, bank accounts, etc., avoid giving out confidential information over the internet and creating difficult-to-guess passwords, combining numbers, uppercase and lowercase letters, and special characters.

BIBLIOGRAPHIC REFERENCES

Abdel-Baset, M., Chang, V., Gamal, A., & Smarandache, F. (2019). An integrated neutrosophic ANP and VIKOR method for achieving sustainable supplier selection: A case study in importing field. Computers in Industry, 106, 94-110. https://reader.elsevier.com/reader/sd/pii/S0166361518307243?token=19595E19694476CDD63F27638BE9A78F54BE8E6DDFD0BE01963F602D5C55618B8A0F2B93F2B4940A8ECBD7B61DD76FF2&originRegion=us-east-1&originCreation=20220818183105

Abdel-Basset, M., & Mohamed, M. (2021). Multicriteria group decision making based on neutrosophic analytic hierarchy process: Suggested modifications. Neutrosophic Sets and Systems, Vol. 43, 2021, 246. https://books.google.es/books?hl=es&lr=&id=UIxCEAAAQBAJ&oi=fnd&pg=PA246&dq=Multi-criteria+group+decision+making+based+on+neutrosophic+analytic+hierarchy+process:+Suggested+modifications&ots=zLQVLcoczq&sig=KkocELyQiJWmEuuJuJ27fPtFpEM#v=onepage&q=Multi-criteria%20group%20decision%20making%20based%20on%20neutrosophic%20analytic%20hierarchy%20process%3A%20Suggested%20modifications&f=false

Acosta, M., Benavides, M., & García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia, 25(89), 351-368.

Cisnero, C., Jiménez, R., & Miranda, L. (2020). Neutrosophic Analytic Hierarchy Process for the Control of the Economic Resources Assigned as Alimony (Vol. 37). Infinite Study.

Ecuador. Asamblea Nacional. (2014). Codigo Organico Integral Penal. Registro Oficial Suplemento N. 180. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

López, J. (2020). La pluralidad de víctimas derivada de la elevada lesividad en los ciberdelitos: una respuesta penal proporcional. Estudios de Deusto, 68(1), 201-221. https://revista-estudios.revistas.deusto.es/article/view/1822/2206

Miro, L. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. IDP: revista d'Internet, dret i política, (32), 1-17. https://raco.cat/index.php/IDP/article/view/n32-miro/473802

Núñez, F., & Carhuancho, B. (2020). Cyber crime in times of covid-19: violation of constitutional rights?. Universidad Femenina del Sagrado Corazón.

Opricovic, S., & Tzeng, G. H. (2007). Extended VIKOR method in comparison with outranking methods. European journal of operational research, 178(2), 514-529.

Paronyan, H., Carballido, R. M., & Matos, M. A. (2020). Neutrosophic VIKOR for Proposal of Reform to Article 189 of the Integral Criminal Code in Ecuador (Vol. 37). Infinite Study.

Peralta, M., & Aguilar, D. (2021). La Ciberseguridad y su concepción en las PYMES de Cuenca, Ecuador. Contabilidad y Auditoría, (53), 99-126. https://ojs.econ.uba.ar/index.php/Contyaudit/article/view/2061/2797

Saaty, T. (2001). Decision making for leaders: the analytic hierarchy process for decisions in a complex world. RWS publications. https://books.google.es/books?hl=es&lr=&id=c8KqSWPFwIUC&oi=fnd&pg=PT8&dq=T.+L.+Saaty,+Decision+making+for+leaders:+:+RWS+Publications,+2014&ots=2MQLJnANOp&sig=U6NLErUg8zTfqGx1LrVzaqt8TxY#v=onepage&q&f=false

Saltos, M., Robalino, J., & Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. Conrado, 17(78), 343-351.

Zambrano, K., & Ordoñez, L. (2016). Delito Informático. Procedimiento Penal en Ecuador. Dominio de las ciencias, 2(2), 204-215. https://dialnet.unirioja.es/descarga/articulo/5761561.pdf