Fuzzy Systems and Data Mining VI
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA200716

Security and Privacy in Information Management in a Distributed Environment for Public Organizations

Segundo Moisés Toapanta Toapanta[1*], Yaritza Julieth Terán Terranova[1], Bertha Alice Naranjo Sánchez[1], Luis Enrique Mafla Gallegos[2]
[1] *Computer Science Department, Salesian Polytechnic University of Ecuador (UPS), Chambers 227 and June, Ecuador*
[2]*Faculty of Systems Engineering, National Polytechnic School (EPN), Ladrón the Guevara E11·253, Ecuador*

Abstract: Security and privacy problems in information management are evident in public organizations. The objective of this research is the analisys risks that these organizations run, since computer attacks have increased along with both internal and external threats. Causing information and database thefts, there are risk analysis methodologies which are oriented to the objective for the preservation of guaranteeing the security and privacy of the information. Were used the deductive method and exploratory research to analyze the articles in the references and in the information available online and MAGERIT methodology what protects the information in its integrity, confidentiality and availability guaranteeing the security of the system and processes of public organizations. It turned out a Control of Security and Privacy factors, Threat Probability, Risk Assessment Formula, Prototype of Risk Management for Public Organizations and Privacy and security factor formula. It was concluded that MAGERIT is an alternative what allow mitigate the vulnerabilitys, threat and risks its processes in public organizations for protecting their information.

Keywords:Management, Distributed Environment, Public Organizations, Privacy and Security.

1. Introduction

Information security represents a great challenge to all organizations, as information is required to be confidential. This research is made on public organizations that currently present information risk problems due computer attacks and internal and external threats. It has been allowed in public organizations, that false and useless information enters with no protection and cause damage and hacking of information and databases. This is why they give higher priority to the protection of their information assets to generate confidence in the citizens, in their environment and in turn prevents them from having risks of computer vulnerabilities [1].

Public organizations face many threats that can affect them. It has been suggested that if the organizations knew and apply the methodology they would not be questioned. The security and privacy of their information and their database would be protected. This is why this article will reveal the help provided by this methodology, it

[*] Corresponding Author: Segundo Moisés Toapanta Toapanta, Salesian Polytechnic University of Ecuador (UPS), Ecuador; Email:stoapanta@ups.edu.ec

is important to take into account the recommendations on this model since it is considered a timely way to help when public organizations faces risks that affect them. Methodology to ensure information security in a distributed architecture for a public organization of Ecuador [2], Hyperledger technology in public organizations in Ecuador [3], Study of the evolution of information security in Colombia: 2000-2018[4], Information security methods to protect rest web services communication and data in http requests using json web token and keycloak red hat single sign on[5], El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados[6], Security of networks and information systems in the European Union: A comprehensive approach? [7], WSN security applied to smart metering systems based on cryptography techniques [8], The reduction of number of parliamentary members and the modification of remuneration schemes for deputies in autonomous community [9], A new data protection law [10], From «computing freedom» towards the constitutionalization of new digital rights (1978-2018) [11], Securing the human: Broadening diversity in cybersecurity[12], Intruder attacks on wireless sensor networks: A soft decision and prevention mechanism[13], Transposition of EU network and information security directive into national law[14] and An Approach to Optimize the Management of Information Security in Public Organizations of Ecuador [15].

The projects implemented in regards to ISO information security and privacy management system, ensure the information assets of public organizations, therefore it is necessary not only the use of methodologies but also of experts who can manage them as it is not rare to see, that these problems harm the security of information on such organizations. Therefore, after the analysis, correct decisions on confidentiality, integrity and availability will be taken. This guarantees improvements in the information security and privacy managing. Looking to optimize it public organizations[15].The MAGERIT methodology finds inconsistency in the organization system, which hasn't been detected before and for a long time, they did not know of their existence. To arrive to the conclusion analysis, we compared with the investigations. This methodology helps to public organizations to have greater control of threats. As a result, security measures were taken, so that they can have a guarantee and that their processes could be manageable, using risk assessment and threat probability formula, a risk management prototype for public organizations and a privacy and security factor formula.

2. Materials and Methods

The procedures used are supported by the reviews of references and articles. It is presented in sequence so to give logical results.

2.1 Materials

The methodology that was used, allowed the correct use of risk analysis, ensuring and protecting the information security and privacy in public organizations with the aim of protecting the database and information within organizations. This is why the MAGERIT methodology was analized; being a risk analysis and management methodology for information systems, known in the European Information Network Security Agency; the methodology used the impacts organizations normally have when security breaches occur and identified the threats that affected these organizations.

Once the vulnerabilities were identified, they could be used to set clear and corrective measures. Technology moves constantly, that is why this methodology helped and will help because it minimize the associated risks, making use of confidentiality, integrity and availability systems that generate trust. This methodology was widely used, without dismissing CRAMM methodology. This analysis and central computer and telecommunications risk control methodology also identified and reduced the attacks that organizations faced. Such methodology relied on the management tool which makes organizations have a clearer vision and be effective acting when facing the threats, previously mentioned [1]. These methodologies were analyzed, approved and were taken into account based on the risk analysis. They found vulnerabilities, threats and risks, allowing better results and providing information security and privacy in public organizations. Risks were analyzed, this being a management tool for decision-making that corrected risks, for improvements and prevention of active analyzes that were factors of the computer systems that support the mission of public organizations, that were threatened causing them damage.

2.2 Methods

The deductive method was used, including criteria applications of the Information Management System (ISMS) that corresponds to ISO / IEC 2700, and risk analysis studied by the research.

2.2.1 Risk Analysis

The security and privacy of the information risks affected entirely to the public organizations. As this methodology determined the threats to which they were exposed, it proved to be effective against these risks that impacted them. Having these factors exposed to threats caused some impact degradation with a certain probability of risks.
In fact, this analysis identifies relevant assets such as information data, computer equipment, information support, communication networks and services. It depended on these types to be able to safeguard threats.
The information system updates constantly, and it also faces more threats. We look to protect the information assets by implementing security control measures, which allow to manage and reduce risks, to achieve the major goal, which is to protect it from threats and risks.

Carrying out the analysis we have the types of risks and threats, in the threats we have of intentional and unintentional types; in the case of the intentional ones in the public organizations the production of damages is tried like the robbery of the information applying the trashing, the malicious codes, impersonation on the other hand in the unintentional ones it is where the actions or omissions take place that if we realize they do not look for to exploit a vulnerability, but that they put in risk the assets of information that this produces a damage like threats related to the natural phenomena. Public organizations should bear in mind that these threats are a warning that damage is imminent, or that damage is occurring or has occurred. Among the risks we have when working in computers without antivirus is possible to have a malware through USB memory most of these are computer viruses, trojans and worms, opening suspicious emails because cybercriminals take advantage of this way in public organizations through users for the theft of information, introduce infected USB flash

drives that is also a risk because possibly someone can collect information, passwords and can collect information from users and confidential information.

2.2.2 Risk management process

Risk management is structured with an ISO standard and we show the following picture

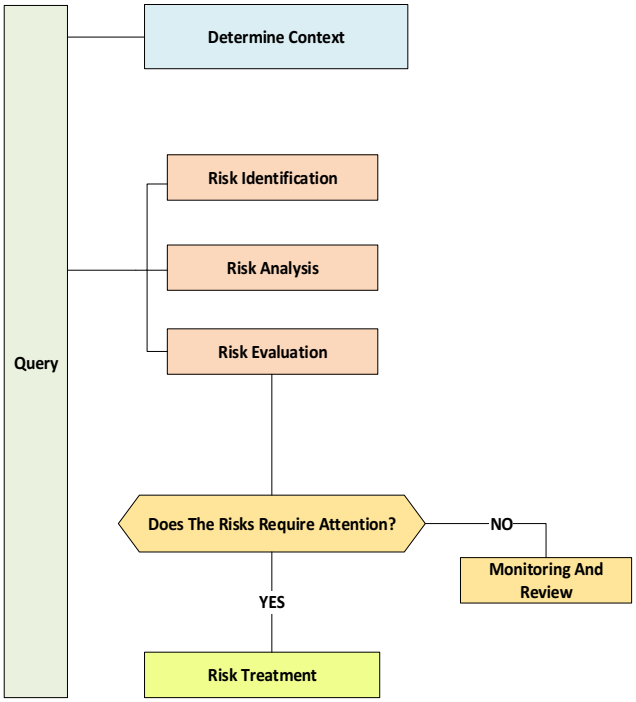

Figure 1. Risk management process

In figure 1, the context is determined, looking for parameters, whether internal or external. We also identify the risks and dangering positions. If they are not identified, they remain hidden. When analyzing the risk it is important to have a vision to which we want to reach and focus on the important risks, executing an evaluation and a treatment represented by analyzed options. At the end, a follow-up and review take place and the incidents are acted on accordingly to observe the continuous improvement in the environment by means of experiences.

With 2 essential things, information that it handles and the services that public organizations provide. Setting requirements for security and privacy of the information in management of the organizations, which are being analyzed, in order to come to an agreement and a stable methodology to avoid that the threats grow but rather minimize them.

2.2.3 *Probability of threats and risks*

Table 1: Risks

High risks	Medium Risks	Low Risks
(12-16)	(8-9)	(1-6)

EXTENT OF DAMAGE				
	4	8	12	16
	3	6	9	12
	2	4	6	8
	1	2	3	4
	LIKELIHOOD OF THREATS			

Table 1 indicates the probability of damage and risk, this being the most used method in risk analysis. We have values as: 1 = Insignificant, 2 = Low, 3 = Medium and 4 = High.

Observing the risk table, the instances it handles and the measure of damage they can cause, the changes that must be made for the best way of handling information are determined. In this process, when analyzing the risks, it is important to have in mind the characteristics of these risks, being those, dynamic and unsteady (perform an interaction between threats and vulnerability), separated by different letters, not always is perceived in the same way between public organizations, so it can produce inadequate results. This method was applied in different public organizations. The higher the probability of threat and magnitude of damage is, the greater the risk and danger to information security and privacy, which means it is mandatory to implement the information security and privacy protection measure.

2.2.4 *Risk analysis methodology*

One of the factors that was taken into account in the organizations, was information privacy and security due the many times some active incidents put them at risk. That is why it is urgent to have variables for the analysis of information security risks.

Table 2: Variables applied to risk analysis

Assets	Threats	Vulnerabilities
Servers	Hacker	Unnecessary open ports
Database	Loss of information	Backup not active
Antivirus	Virus	No antivirus update
Switch	Electric shock	Without preventive maintenance
Firewall	Lack of update	Lack of updates
Technological equipments	Hardware damage	No preventive maintenance

3. Results

The result turns out into a control of security and privacy factors, a risk and probability evaluation formula, a risk management prototype in public organizations and a privacy and security factor formula with the corresponding equations by which it was made known through the analysis provided. The analysis of risk determined by its probabilities allows to have a risk evaluation, to make a global analysis of the risks that need to be prioritized, thus facilitating the decision of the organization to treat and implement the variables related to the analysis of risks.

a) Control of Security and Privacy Factors

It is important to do not lose the sense of the organizational information related to the privacy and security of the given action. To demonstrate this, we convert it in a simple way into graphics. The data shown below has been processed and displayed; it includes details and technical knowledge that perform the main work within the ISMS, to help to make decisions and the necessary adjustments to achieve the aforementioned objectives.

Table 3. Control of Privacy and Security Factors.

Incidents	11
Violations	17
nonconformities	20

In table 3. Description of Privacy control and security factors, giving an referential value to which each one of them can reach. Below, you will find a table and a graphic with indicator data.

Table 4. Monthly privacy and security control

MONTHS	Incidents	Violations	Nonconformities
January	1	3	1
February	2	5	4
March		1	
April	1		
May	3	4	3
June			2
July		2	1
August	1		
September	2		5
October		2	3
November	1		
December			1

In table 4. Monthly Description of the control taken over the privacy and security factors, indicating the incidents, violations and non-conformities that are recorded every month. The monthly control for organizations was presented initially

through measurements and indicators. For information security, we took into account an annual control. In this way through public organizations, the actions taken on information security and privacy were made known.

Table 5. Experimental data of busisness

BUSISNESS	YEAR	USERS
AOL	2006	6.5
DPE	2007	3.2
HPS	2008	134

In the table 5 shows the risk and threat attacks that public organizations had in 3 years, where millions of records were lost by which users are affected.

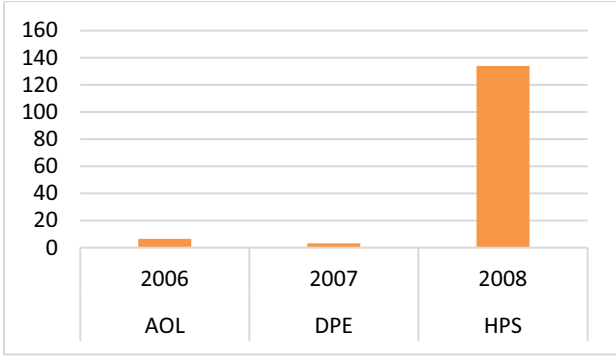

Figure 2. Experimental Data

In figure 2, we have internal attacks, the incidents of information security being these since 2007 in organization DPE (Public Defender's Office of Ecuador) specifying that more than 3.2 million records of clients were stolen in which they include the banking data and the credit cards with personal data the ministry of telecommunications realized the analysis of which they realized the leak of data, on August 6, 2006 there was an attack to AOL, 6.5 million users were affected because their bank details were filled with purchases on a web page, without leaving behind the 2008 attack on the Heartland Payment Systems database, 134 million credit and debit cards were exposed, which resulted in the theft of identity information and money[6].

b) Threat Probability and Risk Assessment Formula

There are several methods of how to assess a risk, many times they are difficult to specify, but it was developed using a mathematical formula.

Values
1 = insignificant, 2 = Low, 3 = Medium y 4 = High
R = Risk, PA = Probability of threats y MD = Magnitude of damage

$$R = PA - MD \quad (1)$$

To represent the risk result, we use the graphic detailed in **Table 1**, in which the x-axis (Probability of threats), and the y-axis (magnitude of damage) can be between 1 Insignificant and 4 High. Facilitating spreadsheets, specifying or estimating the

conditions of the values, providing a risk analysis that allows to give them a position and learn the influence these factors can have in a negative or positive way. To establish the risks in the information security, we did a comparison between the risk probability analysis and its impact. It presents a way to measure the risks according its level of impact and the probabilities established, in the risk zones, presenting also the way to handle that risk.

3.1 Prototype of Risk Management in Public Organizations

The following prototype displayed in the flow chart, show the process steps used to identify risks, in public organizations in order to improve whether internal or externally, preventing or reducing the risks known within the organization, reviewing the need being this, a previously analyzed planning. It gives an alternative to reduce risks on the information security and to improve the management of it. This is why the public organizations take into account the identification of risk to take measures, to supply the necessary resources and implement actions so that after the verifications, the risk management improves, due to the measures taken to improve the security and privacy of information.

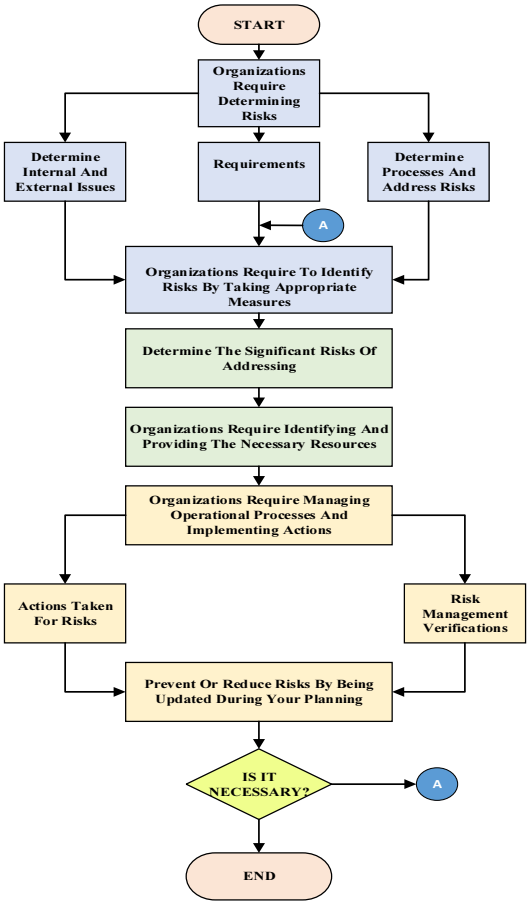

Figure 3. Risk Management Prototype

In figure 3 the risks in the organizations are determined, questioning internally and externally having requirements by which it determines the processes and treats the risks or threats, the public organizations identify the risks taking measures on the analysis that is carried out to be able to do so. Addressing, identifying and providing necessary resources, the operational processes manages and implements actions, whether these are taken for risks, since it prevents and reduces them, being updated during their planning, if it is not necessary to return to identify the processes, but if it is, it ends.

3.2 Privacy and security factor formula

In order to get this results, the factors were taken into account, to help to define clearly the weekly, monthly, quarterly, annually intervals. For this you must; K = Total of factors to evaluate and k = How many are met.

$$\frac{k}{K} = \frac{7}{10} = 0.7 = 70\% \qquad (2)$$

Referring to an example of 10 predetermined factors, 7 are met. using values **Table 3.**

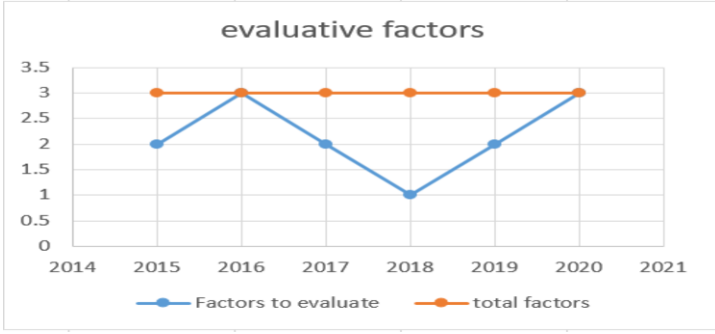

Figure 4. Evaluative factors

In Figure 4 we learn about the factors that need to be evaluated in the last 5 years, remembering that these factors are incidents, violations and non-conformities that exist within public organizations, so good security has not been maintained.

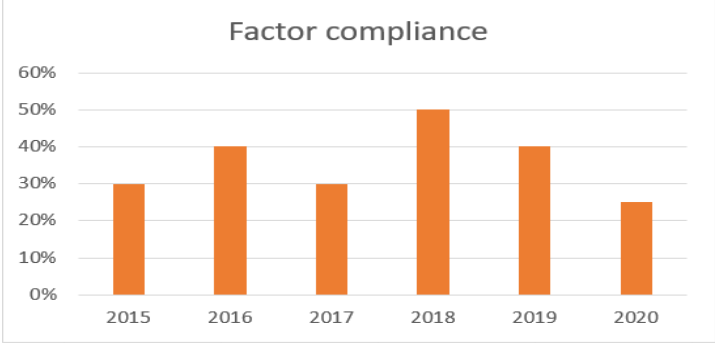

Figure 5. Factor compliance

In figure 5 we have the percentage of compliance of the last 5 years given with the interval formula using K y k.

Table 6. Qualitative Comparisons of proposals

Investigation	Proposition	Factors	Conclusions
[1]	MAGERIT	Confidentiality, integrity and availability	Better results to avoid risks and threats
[3]	Hyperledyer	Advances in technologies	Innovations through open source.
[3]	Blockchain	Organizational Verification	Transparency
[13]	Antivirus	Protection	Prevents damage to the base and protects security.
[15]	ISO	Optimize security management	Information security

Table 6 presents a comparison describing all the analysis carried out and presenting proposals for the security and privacy of the information, making the analysis available and effective.

4. Discussion

It is important that with this research, public organizations have received correct information so that they can follow the methodology and adapt it. It also helped solving information security problems. The methodology should have been taken into account despite the fact, the former methodology didn´t stop threats or risks to damage the information in the database. For this reason, the MAGERIT methodologies analyzed and helped in a qualitative and quantitative way, based in elements such as confidentiality, integrity and availability.

It is then considered that this methodology is the correct and effective alternative to handle information privacy and security in public organizations, without forgetting the ISMS contribution in showing the associated security controls and benefits, determining the main risks and approaches for risk management, which were adjusted to the privacy and security requirements for public organizations.

The results obtained are directly linked to other researches regarding; that for each El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados[6] and An Approach to Optimize the Management of Information Security in Public Organizations of Ecuador [15].

Any prototype based on a methodology must be considered as an alternative for the security and privacy of information in public organizations

5. Future Work and Conclusion

The organization that considers the Prototype Conceptual Model of Security and Privacy of information; it must carry out the analysis of organizations to improve security using the MAGERIT methodologyOrganizations that consider the risk

management prototype in public organizations must determine internal and external risks by identifying and taking the correct measures.
It was concluded that MAGERIT is an alternative what allow mitigate the vulnerabilitys, threat and risks its processes in public organizations for protecting their information.
It was concluded that MAGERIT is a security measure that mitigates the vulnerability, threat and risks of its processes in public organizations to protect information.
The Risk Management prototype and the threat probability and risk assessment formula presented as results are an alternative that improves the security and privacy of information in public organizations.

Acknowledgments

The authors thank to Universidad Politécnica Salesiana del Ecuador, to the research group of the Guayaquil Headquarters "Computing, Security and Information Technology for a Globalized World" (CSITGW) created according to resolution 142-06-2017-07-19 and Secretaría de Educación Superior Ciencia, Tecnología e Innovación (Senescyt).

References

[1] M. A. Tejena-Macías, "Análisis de riesgos en seguridad de la información," *Polo del Conoc.*, vol. 3, no. 4, p. 230, Apr. 2018, doi: 10.23857/pc.v3i4.809.

[2] S. M. T. Toapanta, F. G. M. Quimi, K. E. O. Pazmiño, R. M. Arrellano, and L. E. M. Gallegos, "Methodology to ensure information security in a distributed architecture for a public organization of Ecuador," in *Frontiers in Artificial Intelligence and Applications*, Oct. 2019, vol. 320, pp. 933–944, doi: 10.3233/FAIA190267.

[3] S. M. Toapanta Toapanta, T. F. Prado Quintana, M. R. Maciel Arellano, and L. E. Mafla Gallegos, "Hyperledger technology in public organizations in Ecuador," in *Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020*, Mar. 2020, pp. 294–301, doi: 10.1109/ICICT50521.2020.00052.

[4] J. J. Cano M. and A. Almanza, "Study of the evolution of information security in Colombia: 2000-2018," *RISTI - Rev. Iber. Sist. e Tecnol. Inf.*, vol. 2020, no. E27, pp. 470–483, Mar. 2020.

[5] C. Muyón and F. Montaluisa, "Information security methods to protect rest web services communication and data in http requests using json web token and keycloak red hat single sign on," *RISTI - Rev. Iber. Sist. e Tecnol. Inf.*, vol. 2020, no. E29, pp. 198–213, May 2020.

[6] A. Bogantes, "El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados," in *CICIC 2020 - Decima Conferencia Iberoamericana de Complejidad, Informatica y Cibernetica, Memorias*, 2020, vol. 1, pp. 57–62.

[7] M. Robles Carrillo, "Security of networks and information systems in the European Union: A comprehensive approach?," *Rev. Derecho Comunitario Eur.*, no. 60, pp. 563–600, May 2018, doi: 10.18042/cepc/rdce.60.03.

[8] L. Valencia, T. Guarda, G. P. L. Arias, and G. N. Quiña, "WSN security applied to smart metering systems based on cryptography techniques," *RISTI - Rev. Iber. Sist. e Tecnol. Inf.*, no. E17, pp. 393–406, Jan. 2019.

[9] R. S. Cristóbal, "The reduction of number of parliamentary members and the modification of remuneration schemes for deputies in autonomous community," *Rev. Derecho Polit.*, vol. 92, pp. 73–118, 2015.

[10] A. Rallo Lombarte, "A new data protection law," *Rev. Esp. Derecho Const.*, vol. 2019, no. 116, pp. 45–74, 2019, doi: 10.18042/cepc/redc.116.02.

[11] A. R. Lombarte, "From «computing freedom» towards the constitutionalization of new digital rights (1978-2018)," *Revista de Derecho Politico*, no. 100. Universidad Nacional de Educacion a Distancia, pp. 639–669, Sep. 01, 2017.

[12] M. Azhar *et al.*, "Securing the human: Broadening diversity in cybersecurity," in *Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE*, Jul. 2019, pp. 251–252, doi: 10.1145/3304221.3325537.

[13] I. Hussain, S. Zahra, A. Hussain, H. D. Bedru, S. Haider, and D. Gumzhacheva, "Intruder attacks on wireless sensor networks: A soft decision and prevention mechanism," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 5, pp. 609–617, 2019, doi: 10.14569/ijacsa.2019.0100578.

[14] T. Katulic, "Transposition of EU network and information security directive into national law," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2018 - Proceedings*, Jun. 2018, pp. 1143–1148, doi: 10.23919/MIPRO.2018.8400208.

[15] S. Moisés Toapanta Toapanta and L. Enrique Mafla Gallegos, "An Approach to Optimize the Management of Information Security in Public Organizations of Ecuador," in *Fault Detection, Diagnosis and Prognosis*, IntechOpen, 2020.