Analysis of New Technologies in Information Security to Mitigate Data Risks in a Public Organization

*Segundo Moisés Toapanta Toapanta
Department of Computer Science
Salesian Polytechnic University (UPS)
Guayaquil, Ecuador
stoapanta@ups.edu.ec

Luis Enrique Mafla Gallegos
Faculty of Engineering Systems
National polytechnic school (EPN)
Quito, Ecuador
enrique.mafla@epn.edu.ec

Mario Darío Medina Lara
Department of Computer Science
Salesian Polytechnic University (UPS)
Guayaquil, Ecuador
mmedinal@est.ups.edu.ec

Javier Gonzalo Ortiz Rojas
Department of Computer Science
Salesian Polytechnic University (UPS)
Guayaquil, Ecuador
jortiz@est.ups.edu.ec

***Abstract*— Were analyzed references on alternative technologies or new proposals to help mitigate data risks. The problem is the lack of application of new technologies that secure information and reduce risks in organizations. The objective is to perform an analysis of new technologies in information security to minimize the risks of data in a public organization. It was used deductive method and exploratory research were used to analyze the information of the referenced articles. It turned out: Mixed Conceptual Model of Information Control, Double Security Architecture for Public Organization in Educational Area, Algorithm Control of Information Security. It was concluded that blockchain is considered as a fundamental option to provide control, robustness against failures and malicious attacks, reliability, availability, immutability and security.**

Keywords—New technologies; Mitigate the risks; Foreign trade; Information security.

I. INTRODUCTION

The security holes in the software are common and the problem is increasing; leverages software engineering best practices and tries to make people think about security from the first moment of the software life cycle; the security of this is the set of preventive and reactive measures of organizations that allow to safeguard and protect information in order to maintain confidentiality, availability and data integrity; and the concept of information security should not be confused with that of computer security,since the latter only takes care of the security in the computer environment [1]. The field of information security has grown and evolved considerably, becoming a globally accredited sector; and this field offers many areas of expertise, including auditing information systems, planning business continuity, digital forensic science and managing security management systems; includes various aspects including availability, communication, problem identification, risk analysis, integrity, confidentiality, risk recovery [2].

The rapid evolution of the internet of things, considers that organizations have made progress in relying on their protocol systems and networks; however, this issue also generates many new information security problems [1]. Edward Snowden's results on countless foreign intelligence surveillance activities led countries such as Indonesia to take enhanced protocols for the security of classified data and their communications; an adaptive broadband Delphi study was implemented to explore and mitigate the surveillance activities of the Five Eyes (United States – United Kingdom – Canada – Australia – New Zealand); where the agency security method was used three elements of defense in depth (people, operations and technology), in combination with government and legal resources [2].

The main drawback of the public sectors is the inefficient control of resources, where possible, in which one organizations can generate a contract with one or more parties; it must be filtered by a somewhat cumbersome process in which a third party participates and in this way such contract has reliability and security for the confidentiality of information [3]. The great advancement of an effective awareness of the cyber world, brings significantly to the process and decision-making protocols in information risk management; it is one of the main objectives that organizations manage in sectors, the sending and receiving of such information between and within organizations, was considered a key security enabler [4]. As cybercriminals increase their attacks, computer security reaches a greater degree of sophistication; the system generates reputation information for network resources such as IP, URL, and hash file files found in selected security data from security information systems and event management; Cyber Threat Intelligence is a knowledge-based alert management system that encompasses increased cyber threats [5]. There are several types of computer security that a company must monitor to prevent data loss and/or prestige; and real-time information sharing across organizations provides new opportunities to improve information infrastructures and security [6].

978-1-7281-7283-5/20/$31.00 ©2020 IEEE
DOI 10.1109/ICICT50521.2020.00049

Why is it necessary to perform an analysis of new information security technologies to mitigate data risks in a public organization?

The digital transformation process in which most organizations and society in general are immersed, allows attacks on the computer security of companies to be committed from anywhere in the world using as a tool only a computer. This is why organizations have to pay special attention to protect themselves from possible attacks as no one is safe from malware.

The objective is to perform an analysis of new technologies in information security to minimize the risks of data in a public organization.

The articles reviewed are:

An Improved Information Security Risk Assessments Method for Cyber-Physical-Social Computing and Networking [1], An Adaptive Wideband Delphi Method to Study State Cyber-Defence Requirements [2], A Hyperledger Scheme for the Deployment of Smart Contracts in a Public A Hyperledger Scheme for the Deployment of Smart Contracts in a Public Organization of Ecuador [3], Are we managing the risk of sharing Cyber Situational Awareness ? [4], A Reliability Comparison Method for OSINT Validity Analysis [5], Enhancing Privacy of Information Brokering in Smart Districts by Adaptive Pseudonymization [6], Improving information security risk analysis by including threat-occurrence predictive models [7], An Efficient Data-Driven Clustering Technique to Detect Attacks in SCADA Systems [8], A New Metric for Measuring the Security of an Environment : The Secrecy Pressure [9], A Blockchain Approach to Mitigate Information Security in a Public Organization for Ecuador A Blockchain Approach to Mitigate Information Security in a Public Organization for Ecuador [10], Channel-Aware Artificial Intersymbol Interference for Enhancing Physical Layer Security [11], Mihaela Ulieru and Paul Worthington [12], Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage [13], Privacy preservation and public auditing for cloud data using ass in [14], Nano Meets Security : Exploring Nanoelectronic Devices for Security Applications [15], An Approach of Models of Information Technologies Suitable to Optimize Management in a Public Organization of Ecuador [16], Network Diversity: A Security Metric for Evaluating the Resilience of Networks Against Zero-Day Attacks [17], ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO / IEC 27005 [18], New Complementary Points of Cyber Security Schemes for Critical Digital Assets at Nuclear Power Plants [19], A Privacy-Preserving RLWE-Based Remote Biometric Authentication Scheme for Single and Multi-Server Environments [20].

Hyperledger is applied in Smart Contracts, we have Blockchain as the main method; the structure in a blockchain is that a block, consisting of multiple transactions, is connected to a previous block in the form of a string. Smart contracts are a set of scenario-response and logical procedure rules; the results are mostly criteria for information security in systems, which prioritize data integrity and security through encryption and security protocol; the research process was determined by an algorithm scheme using flowchart techniques as an option to mitigate data security in a public organization; the prototype performed, can be used as a reference for other public sector companies.

Deductive method and exploratory research are used to analyze the information of the referenced articles.

The results are: Mixed Conceptual Model of Information Control, Double Security Architecture for Public Organization in Educational Area, Algorithm Control of Information Security.

It is concluded that blockchain is considered as a fundamental option to provide control, robustness against failures and malicious attacks, reliability, availability, immutability and security.

II. Materials And Methods

A. *Materials.*

An improved search algorithm was proposed that previously trained a red neuronal reverse propagation in areas of improving accuracy and stability; this pre-workout protocol, the algorithm was able to advance the defect of making mistakes at local minimums and surprisingly improving its efficiency; this neural network was used as a member of the information security risk assessment processes for a miniature technology; this try with a simulation test to validate the performance of the proposed algorithm; despite the successful development of the proposed method [1].

This article developed broadband to study the Indonesian government's requirements for cyber defense in response to secret intelligence reports in Australia; the key requirements for protection against foreign surveillance that it took into account in state cyber defense frameworks were also described; where effective mitigation controls were suggested to safeguard and protect national interests of states; they developed a variant approach that investigates how governments protect national security and privacy in cyberspace [2].

The purpose of this research was the implementation in the public sector of Ecuador, only in the use of Smart Contracts; the reason why deploying on Smart Contracts in an organization in the aforementioned sector is the security offered by Blockchain; having the transaction data being retracted in a red and being this free of income; one of the main advantages of implementing this technology is that it no longer depends on a third or extra part or intermediary for validity in transactions; by representatively minimizing the costs of bureaucracy or third parties, and ensuring the consistency and availability of information; were subjected to changes or alterations depending on the business model of the organization; they deduced that public organizations could be totally managed by Smart Contracts [3].

This document considered a case analysis of a UK public sector organization; its objective was to determine whether the option of sharing awareness of the cyber situation has been taken from an information risk management point of view; it was examined whether the organization was properly located or not, to manage the consequences of the loss of information that was obtained as a result of the data exchange process; According to the author, this case analysis provided relevant evidence to answer the question of whether or not the correct risk management processes protect the selected decisions; to consider raising awareness of the ethical cyber situation between organizations [4].

In this article, we implemented a model that was able to analyze the reliability and validity of the data by using comparative analysis among the base line data; a criterion was presented to assess the reliability of the feed that yielded corresponding data; the experiment used about 40000 datasets to provide precision results of the same for four sources; these results could be used as a basis for substantive validation to use information security data [5].

Security and privacy requirements were observed and an architecture was structured that improves privacy for an information broker age platform; an adaptive pseudonymization framework was presented to prevent and complicate privacy attacks and capture real-time consumer protection of the platforms; to complete an assessment was carried out an evaluation was carried out using real-world energy consumption measurements [6].

This article, an alternative predictive model was proposed for risk analysis methodologies; the proposal is based on a calculation of modification risk by replacing past threat frequencies with likelihood of future threats taking into account the current vulnerabilities of the system; intervention of prediction in risk analysis processes would allow organizations to expand their knowledge of the contexts of their assets in information [7].

An innovative goal of locating intruders to detect attacks was presented; this was formed from a grouping technique based on process parameter data, which quickly and automatically identified the normal and critical states of a given system; then established detection rules based on the proximity of the assigned states for monitoring; a greater satisfaction of tests was achieved by performing countless experiments on eight sets of data sets that included parameter values processes; the results showed 98% accuracy in the automatic identification of critical states, which in turn facilitated system monitoring [8].

The objective was to define a new metric, which is characteristic of the security of the surface or environment where the legitimate link is immersed, regardless of the position of the node listeners; the contribution of this document is twofold: first a framework for the derivation of the capacity of a surface, which considers all the parameters that influence the secret of information capacity; second, the definition of a metric to measure the secrecy of a data surface [9].

In this document analyzed and determined the security problem of Ecuador's public organizations; and the objective was to generate a prototype of blockchain using a flowchart algorithm that facilitated consistency against errors, third-party attacks and mitigated information threats; it proved an algorithm given with flowchart techniques for making advances in information processing in a public organization in Ecuador and the use of the algorithm; it was concluded that the entry into information of a generic public organization in Ecuador had an option to improve information security with the implementation of blockchain [10]. In order to develop this topic, a new scheme was achieved where the security of the transfer of information between devices with limited resources was improved; a set called pulses was selected to shape the data in the source based on the original channel status information; or purpose that in turn had the information channel correctly showed the output of the matching filter; a spy who has no knowledge of the original channel; in addition, the results of the simulation showed that at the difference of the destination, the percentage of symbol error in spy collapsed to a high data due to the induced index [11].

The final point of view of this work was to deploy an adaptive risk management framework capable of cautiously, distinguishing and answering critical time to alerts; the focus was on defending the infrastructure at risk as public services that necessarily depends on the security of the network and information; a holistic system of Cyber security was established; the system was dynamically coupled to accept new risk situations and was able to strategically create and learn risk models as it encountered new risk situations [12].

This article explored the security of a cryptographic primitive; public key encryption with encrypted key search served access on all cloud storage systems; a disadvantage is that it was shown that the traditional framework suffered from an unexpected alert called internal keyword guessing attack that was issued by the malicious server ; for this security attack, it was proposed the same framework with dual server; additional version of the functions was determined; a safe generic structure was also provided to determine the effectiveness of this framework, an efficient instance of the overall framework was provided, proving to achieve safety against the interior [13].

This protocol, the identification of the signer of a set of shared data blocks was killed by public seers; the integrity of the shared data is efficiently analyzed without retrieving the original file; tracking is a major problem; to implement this trace it was used a multi-cloud database scheme that is supported by multi-cloud service providers; or moved towards multiple clouds was highly favorable and this system also validated data that is attacked by malicious users, with a short time and cost requirement [14].

The hardware security based on nano electronics preserved some advantages to the tie that obtained to allow conceptually successful security applications; this tutorial showed how hardware security primitives have been developed achieving the original features, such as complex equipment and system structures; also in this document explained the security capabilities of various emerging nano electronic devices; here the outstanding goals in the use of emerging nano-electronic devices for safety were identified [15].

The objective of this research was to analyze information technology models to improve protocols in a public organization based on its principles and strategic points; he was able to adopt the ITIL model to optimize technological management in a public organization in Ecuador; I know he needed to be with mobile devices to national level that access different network distributors and access necessary information; in addition to meeting the objectives required by public institutions, internal users and external steers [16].

In this document, the first step was made to model network diversity as a safety metric by having designed and analyzed a series of diversity metrics; a biodiversity-inspired metric was structured under the effective number of distinct resources; even two metrics of diversity were raised in the folds, which were designed in the minimum and weighted attack efforts, respectively; it was finished by evaluating the metrics that were proposed through the simulation [17].

Their search proposed a practical guide for the risk management of ICT presented in state entities that complied with ISO / IEC 27005; and this analysis also shared an exemplary and real study of the proposed methodology to show its benefits and applicability [18]. These analysis tests obtained in this article were applied to technical measures for the cybersecurity of critical digital assets in nuclear power plants; technology that was at an appropriate point in cybersecurity ensured technical security; the approach to equating and developing schemes in the cyber security environment; the advantages of the c-points of various cybersecurity protocols identified in such analyses were taken as an advantage [19].

It proposed a remote, original, and efficient biometric authentication scheme they gave smartcard and a public key cryptographic system; it was the first remote, network-based biometric authentication scheme for multiple server environments; all of this security analysis was show to be able to meet the security of authenticated key exchange and the random oracle model, resisting known security attacks; provided in turn back quantum security; this experimental assessment and analysis comparative showed computational efficiency, while the efficiency of communication were less [20].

B. *Methods*

1) *Considerations:*

We propose to use a technique to store information safely and permanently with tracking features, such as blockchain, we also propose to use an information management protocol; by combining these two new technologies in public organizations we will have a model to mitigate the risks of information.

2) *Comparative table:*

We made Table I to get a better view of the references, presents the technology that the authors were based on and a description of the proposal.

Table I provides a brief description of each of the articles that was taken as a reference for the analysis of new technologies; in this way the process can be visualized in brief detail along with its method.

TABLE I. ARTICLE COMPARISON

Reference	Technology	Method or process
[1].	Neural Network Search Algorithm.	Using a reverse-propagation neural network as a component of the evaluation process.
[2].	Inter-Organization Data Response Network.	Communication via cyberspace with security protocols and parameters.
[3].	Model based on Blockchain structure.	It is processed independently, without relying on intermediaries to share the information.
[4].	Information Sharing Risk Protocol	Use of lost data for improved data exchange.
[5].	Data Reliability Model.	Data is handled for comparative analysis between bases.
[6].	Information Platform Architecture.	Adaptive framework that prevents attacks and threats to protected data.
[7].	Predictive model.	Using past risks to prevent future risks and provide information security.
[8].	Intruder Location Protocol.	Monitor the states assigned to processes to analyze threats to data.
[9].	Information Surface Security Metrics.	It generates an information security framework on the platform to measure your bearable rate.
[10].	Blockchain prototype.	Flowchart algorithm that facilitated consistency against errors.
[11].	Data Transfer Security Scheme.	A set of information called pulses is taken to shape the base.
[12].	Adaptive Risk Management Framework.	Use of a holistic system of Strategic Security.
[13].	Frame structure with Double Feed.	Assigning Instances within the Server for Data Security.
[14].	Shared Data Identification Protocol.	Multiple databases are involved and it tracks malicious attacks.
[15].	Physical Technology for Nano-based Security.	Proceeds to implement security to several nano-electronic devices.
[16].	Models of Improvements in Security Protocols.	Review of ICT-related information implemented.
[17].	Data Resource Security Metric.	Based on Software Instances with Collected Information Simulation.
[18].	Information Risk Management Process Guide.	Adopts ISO/ICE 27005.
[19].	Security Methods and Protocols for CyberAttacks.	Analysis Results on Nuclear Plant Critical Data Systems.
[20].	Authentication Equipment Scheme.	Using smart cards for key exchange security.

III. RESULTS

We propose the following results:

- Mixed Conceptual Model of Information Control.
- Double Security Architecture for Public Organization in Educational Area.
- Algorithm Control of Information Security.

A. *Mixed Conceptual Model of Information Control.*

The proposed model for analyzing new information security technologies to mitigate data risks in a public organization is:

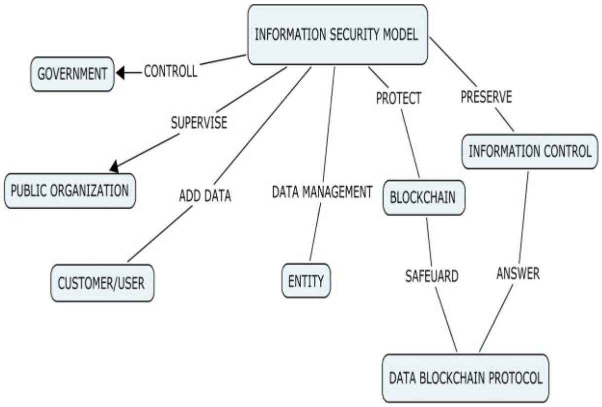

Figure 1. Conceptual model.

Fig. 1 shows the conceptual model of Information Security and exchanges data with the relevant government entity for the quick handling of any type of transactional action; in this model we can visualize how each actor has its function related to the management of its operations; blockchain is added to encrypt the corresponding data together with an information control model; together they form a blockchain protocol of data; the purpose of this model is to be able to establish an improvement relationship with technologies based on information security; access to the platform is validated according to the public organization to define which source is reliable and to safeguard and give access to relevant information.

For the calculation of the measurement of the conceptual model presented, we have made the following formula (1):

$$Mmc = 1 - \frac{ADBU}{APO + ACO + APC + AIBU} \quad (1)$$

Here:

APO, amount of dependency of the public organization.

ADBU, amount of direct beneficiaries of each unit.

ACO, amount of control office.

APC, amount of people by control office.

AIBU, amount of indirect beneficiaries of each unit.

Example: for the coastal region in the province of Guayas, a measurement of 97.62% was established; for Manabí province, 82.99%; for the province of Santa Elena 98.77%; for the province of El Oro 94.34%; for the province of Los Ríos 84.03%; and in the province of Esmeralda 90.03%.

Fig. 2 shows the measurement percentages of each province of the coastal region, taking indicator indicators for measurement; this allows you to have a view of the comparisons at the percentage level of each place.

B. *Double Security Architecture for Public Organization in Educational Area.*

It proposes an architecture for a public organization in this case in the educational area; it establishes the participation of 5 actors as student, teacher, academic entity, government, and the public organization that is the ministry of education; these participants have an individual function such as platform management, registration application, configuration management, control and monitoring in the interconnection process; in carrying out this process with their due actions is carried out comes to the entrance of the Blockchain encrypted data structure; once this process is done, a secure and complete data transmission is established without having malicious information and thus the organization publishes having greater security in its data.

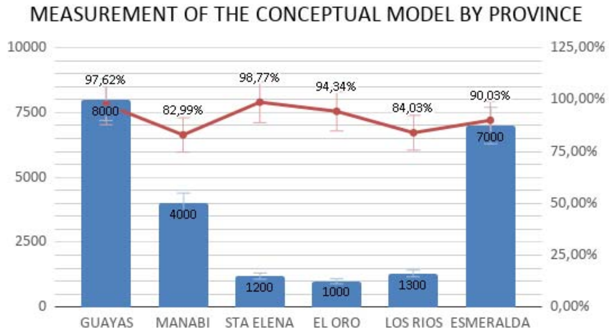

Figure 2. Measurement Chart of the Conceptual Model

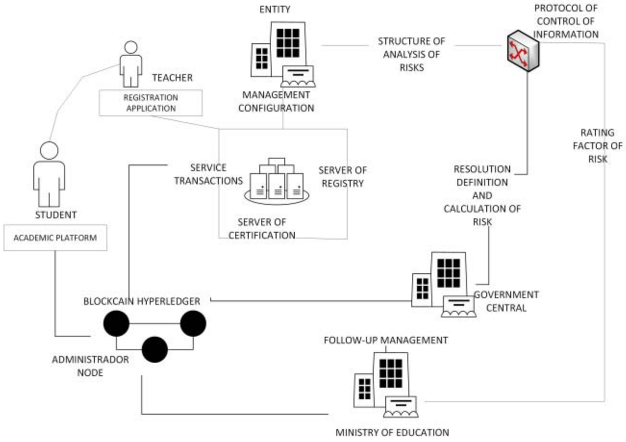

Figure 3. Architecture Proposal for Public Organization - Educational Area.

Fig. 3 shows the connection of the two technologies to mitigate data risks; the Information Control protocol applies risk assessment structuring to the state entity that generates the information in detail to the blockchain; risk factor assessment is applied in the public organization in this case to the Ministry of Education which also generates summary information to the blockchain; risk resolution and calculation is applied by the central government which will be indicators that are recorded on the blockchain.

The blockchain architecture is proposed for the following reasons: the information is immutable, you can perform an audit of the information, the data remains encrypted; there is a consensus among participants when updating information, participants have an authentication certificate; all actors such as the public organization and the government will have a copy of the information in blockchain; the academic entity is authorized to enter information related to the management of its area; students have a general identifier for data querying, teachers have a general identifier for each school for data entry.

It is proposed that blockchain be on the Hyperledger platform, in this case intervene: the central government, the academic entity and the ministry; an authentication is determined to enter the network and update the information if necessary, these actors are the ones who give consent to update the data, that is to say form the consensus.

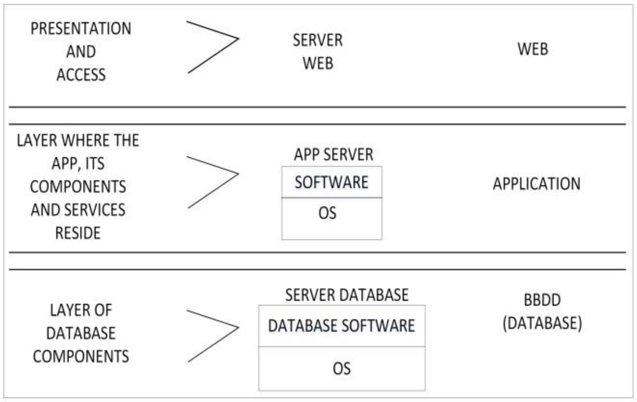

Figure 4. Three Layer Architecture:

Fig. 4 shows the layer structure count of 3 levels to handle each process in a respective way with the exchange of data with the public organization and its participants; the first layer is the so-called "Web Layer", which hosts the web server and runs the presentation and access to the information; we find the entity and the structuring of risk assessment; the second layer named "Application", is the application server, the software, the operating system; implementation of its components and services, valuation actions, resolution and risk calculation are carried out; decision is considered in this layer whether or not the threat is accepted with their respective reactions, i.e. monitors risks, or monitors and minimizes them; and in our latest layer named "BBDD Layer", we maintain the database server, database software and its operating system; is the level of database components and runs the storage of information and its classification for security.

C. *Algorithm Control of Information Security.*

We proposed the if guiding algorithm in the process of analyzing new information security technologies to mitigate data risks in public organizations; the algorithm presented above aims to improve the steps of the methodology to avoid threats in the information.

Fig. 5 describes in phases how to apply the security algorithm to information by starting the structuring of risk assessment; where it is established, methods building assessment groups; continues the assessment of the risk factor, involves the assessment of threats towards the data; as the following action is the risk resolution that determines the vulnerability of threats, severe risk and risk control measures; the risk calculation performs, the risk comparison of the assessment criteria alongside of the range of established risks; as the threat is accepted, the risk is monitored, otherwise it is monitored to minimize the risk; this process culminates with the storage and classification of the same with the prevention of the risks received.

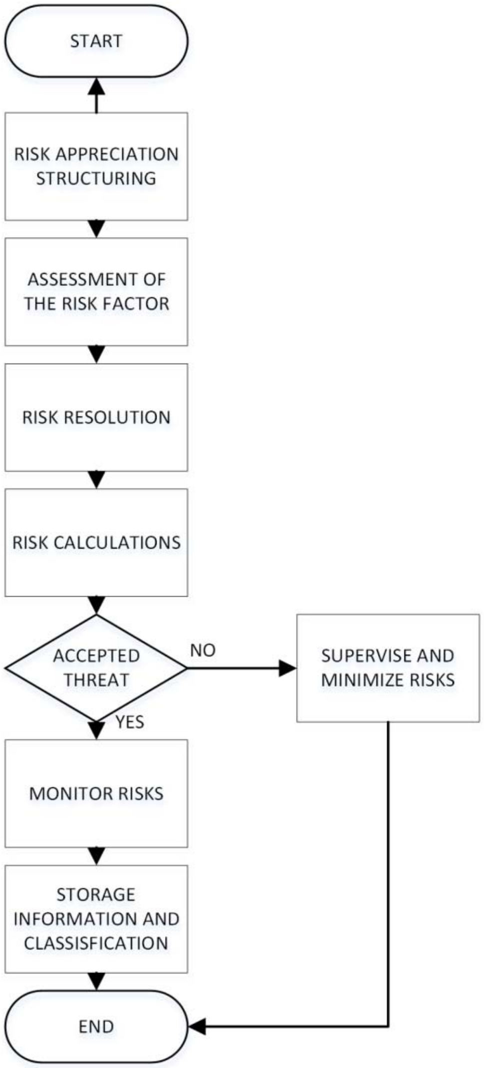
START
RISK APPRECIATION STRUCTURING
ASSESSMENT OF THE RISK FACTOR
RISK RESOLUTION
RISK CALCULATIONS
ACCEPTED THREAT
NO
YES
SUPERVISE AND MINIMIZE RISKS
MONITOR RISKS
STORAGE INFORMATION AND CLASSIFICATION
END

Figure 5. Information control algorithm.

Use Case:

The following use case is adopted with a public organization belonging to the educational area:

1) The risk assessment structuring is determined and criteria are evaluated, the entity related to the public organization is in charge.
2) The assessment of risk factors is determined by the evaluation carried out by the public organization, the Ministry of Education, carrying out its monitoring management.
3) Risk resolution is led by the central government, where tracking and steps for vulnerability, threats and severe risk are carried out.

4) Risk calculation is where the government performs a comparison of the established risk criteria.
5) Decision is made whether or not the risk or threat found is accepted; whether it is not accepted, the process to be taken is to monitor and minimize the risks encountered; if the decision is affirmative, we proceed to monitor the risks, to analyze the future possibilities of data loss.
6) The process in storage and classification is completed, together with measures to prevent risks to data security.

For the calculation of the potentiated risk and minimized risks presented, we have made the following formula (2):

$$Rpm = 1 - \frac{ARC}{RS + ARF + ARR} \qquad (2)$$

Here:
ARC, amount of risk calculation.
RS, risk structures.
ARF, amount of risk factor.
ARR, amount of risk resolution.

Example, for supervised risks 36% is obtained, for 22% monitored risks, minimized risks are 48%, and accepted risks 44%.

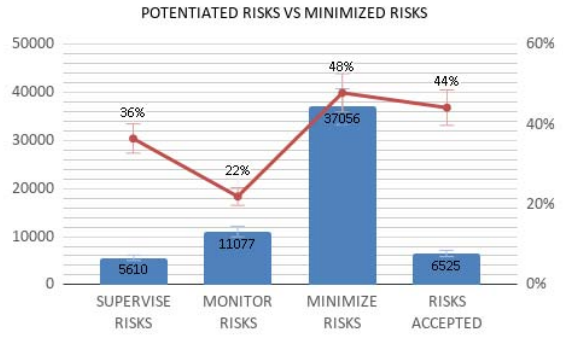

Figure 6. Potentiated Risks vs Minimized Risks.

Fig. 6 in this development of values a margin of percentage comparison is obtained between certain important points of information security.

IV. Discussion

To propose the results in this research we adopt the Reference Blockchain technology[10], to give a higher level of security and consistency to the information that is generated, avoid malicious actions in the management of information; we also adopt the methodology of information control of the reference [1] to collect historical data and mitigate risks in the future through the established protocol.

- The results obtained were mostly criteria for information security in systems, which prioritize data integrity and security through encryption and security protocol.
- In the research process, an algorithm scheme was determined using flowchart techniques as an option to mitigate data security in a public organization; the prototype made can be used as a reference for other public sector companies.
- It was determined that the application of Blockchain has been very revolutionary and enjoys a reputation for its security feature, it can efficiently secure the information it shows to the user; because when technology is combined with another, a new form of digital exchange and security is created so that unexpected information changes do not occur.

V. Future Work and Conclusions

It is suggested that a future research topic be the analysis of information vulnerabilities and risks, the evaluation of each process and available systems; public organizations should do this analysis prior to the implementation of blockchain and protocols as an alternative to improving information security.

From the research carried out, the following can be concluded:

- It was concluded that blockchain is considered as a fundamental option to provide control, robustness against failures and malicious attacks, reliability, availability, immutability and security.
- The algorithm needs to be further improved to minimize certain parameters or processes involving runtime and risk assessment.
- The integrity and accessibility of information in public organizations have a higher priority and security option of the blockchain over confidentiality and authenticity.

It should be considered that the protocols followed in our experiment are fully applicable in other researches that in turn need to delve into the topic of new technologies and methods to mitigate information security risks.

Acknowledgment

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] S. Li, F. Bi, W. E. I. Chen, X. Miao, J. I. N. Liu, and C. Tang, “An Improved Information Security Risk Assessments Method for Cyber-Physical- Social Computing and Networking,” *IEEE Access*, vol. 6, pp. 10311–10319, 2018.

[2] Y. Nugraha, S. Member, and I. A. N. Brown, “An Adaptive Wideband Delphi Method to Study State Cyber-Defence Requirements,” *IEEE Trans. Emerg. Top. Comput.*, vol. 4, no. 1, pp. 47–59, 2016.

[3] J. Espinoza, E. Mafla, and C. Technologies, “A Hyperledger Scheme for the Deployment of Smart Contracts in a Public A Hyperledger Scheme for the Deployment of Smart Contracts in a Public Organization of Ecuador,” no. January, 2019.

[4] M. Davies and M. Patel, “Are we managing the risk of sharing Cyber Situational Awareness ?,” *2016 Int. Conf. Cyber Situational Awareness, Data Anal. Assess.*, pp. 1–2.

[5] S. Gong, J. Cho, and C. Lee, “A Reliability Comparison Method for OSINT Validity Analysis,” *IEEE Trans. Ind. Informatics*, vol. 14, no. 12, pp. 5428–5435, 2018.

[6] J. Suomalainen and J. Julku, “Enhancing Privacy of Information Brokering in Smart Districts by Adaptive Pseudonymization,” *IEEE Access*, vol. 4, pp. 914–927, 2016.

[7] P. Tubío Figueira, C. López Bravo, and J. L. Rivas López, “Improving information security risk analysis by including threat-occurrence predictive models,” *Comput. Secur.*, vol. 88, 2020.

[8] A. Almalawi, A. Fahad, Z. Tari, A. Alamri, R. Alghamdi, and A. Y. Zomaya, “An Efficient Data-Driven Clustering Technique to Detect Attacks in SCADA Systems,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 5, pp. 893–906, 2016.

[9] L. Mucchi *et al.*, “A New Metric for Measuring the Security of an Environment : The Secrecy Pressure,” *IEEE Trans. Wirel. Commun.*, vol. 16, no. 5, pp. 3416–3430, 2017.

[10] M. Toapanta, J. Mero, D. Huilcapi, and M. Tandazo, “A Blockchain Approach to Mitigate Information Security in a Public Organization for Ecuador A Blockchain Approach to Mitigate Information Security in a Public Organization for Ecuador,” 2018.

[11] S. V. Pechetti and R. Bose, “Channel-Aware Artificial Intersymbol Interference for Enhancing Physical Layer Security,” *IEEE Commun. Lett.*, vol. 23, no. 7, pp. 1182–1185, 2019.

[12] M. Ulieru and P. Worthington, “Mihaela Ulieru and Paul Worthington.”

[13] R. Chen, Y. Mu, S. Member, G. Yang, F. Guo, and X. Wang, “Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage,” vol. 11, no. 4, pp. 789–798, 2016.

[14] J. Suganthi, “PRIVACY PRESERVATION AND PUBLIC AUDITING FOR CLOUD DATA USING ASS IN,” *2015 Int. Conf. Innov. Information, Embed. Commun. Syst.*, pp. 1–6, 2015.

[15] J. B. Wendt, S. M. Ieee, M. Potkonjak, N. Mcdonald, G. S. Rose, and B. Wysocki, “Nano Meets Security : Exploring Nanoelectronic Devices for Security Applications,” *Proc. IEEE*, vol. 103, no. 5, pp. 829–849, 2015.

[16] M. Prado and E. Mafla, “An Approach of Models of Information Technologies Suitable to Optimize Management in a Public Organization of Ecuador,” *World Conf. Smart Trends Syst. Secur. Sustain. (WS4 2019)* , no. July, 2019.

[17] M. Zhang, L. Wang, S. Jajodia, A. Singhal, and M. Albanese, “Network Diversity: A Security Metric for Evaluating the Resilience of Networks Against Zero-Day Attacks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 5, pp. 1071–1086, 2016.

[18] S. Patiño, “ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO / IEC 27005,” pp. 75–82, 2018.

[19] J. Son, J. Choi, and H. Yoon, “New Complementary Points of Cyber Security Schemes for Critical Digital Assets at Nuclear Power Plants,” *IEEE Access*, vol. 7, pp. 78379–78390, 2019.

[20] H. Yao *et al.*, “A Privacy-Preserving RLWE-Based Remote Biometric Authentication Scheme for Single and Multi-Server Environments,” *IEEE Access*, vol. 7, pp. 109597–109611, 2019.