ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 5, 352-359 (2019)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Analysis of Information Security for a Voting Process for Sectional Governments in Ecuador

Segundo Moisés Toapanta Toapanta[*,1], Steven Xavier Romo Sañicela[1], Danny Wilfrido Barona Valencia[1], Luis Enrique Mafla Gallegos[2]

[1]*Department of Computer Science, Universidad Politécnica Salesiana (UPS), Guayaquil, Ecuador*

[2]*Facultad of System Engineering, Escuela Politécnica Nacional del Ecuador (EPN), Quito, Ecuador*

ARTICLE INFO

Article history:
Received: 08 July, 2019
Accepted: 08 October, 2019
Online: 22 October, 2019

Keywords:
Electronic in Ecuador
Integrity of the information
Sectional Elections
Security of the information
Voting Processes

ABSTRACT

Knowing about different events in several Latin American countries, as well as in Ecuador, in relation to data alteration, in the different sectional voting processes, it has been necessary to carry out a security analysis provided by the systems of choice in the different sectional governments of the country. The objective of this study is to analyze information security policies, their processes, standards and encryption methods, for the voting processes of the National Electoral Council of Ecuador (CNE). In this study a qualitative, deductive and exploratory research approach was applied, which allowed an analysis of the articles in reference. The articles of law that the Constitution has stipulated were reviewed, since the country manages a traditional system, which is carried out through several stages or phases, but which in turn uses technological tools. During these stages there are risks that can harm the sectional candidates, in such a way that a review of the Ecuadorian reality is essential, which implies the commitment of their actors, working as a team with specialists in the different areas, as well as compliance with public policies. It is concluded that the prevention, processes and policies proposed by the entity are based on the pillars of information security of the ISO 27001 standard, it is also pertinent that the cryptography implemented by the CNE with the hash code is in constant integration with new more robust and secure cryptographic methods providing greater security, integrity and confidentiality avoiding alterations in the data entered in the electoral process.

1. Introduction

The use of technology in different spheres of activity within the country is on the rise, so it can be seen in the area of education, banking, commercial and other state entities, as in the electoral system of the National Electoral Council of Ecuador (CNE). Thanks to these technological advances, implemented in various systems, the voting processes have been expedited, but the risk of information manipulation have also increased, vulnerabilities, threats and risks in the end results.

Electronic voting systems are critical security systems that require early identification of security requirements and controls based on the analysis of potential vulnerabilities, threats, attacks and associated risks[1].

In Ecuador, voting systems in line with the regulatory framework OSI (Information Security Officer), it can be done in two ways which can be both physical or digital, however, the electoral process carried out in the country is maintained with the traditional model. Where results are counted, digitized, stored and presented in real time from the website of the National Electoral Council (CNE), either for presidential elections or the election of sectional rulers.

The need to build an internet presence has motivated governments to develop websites and portals for information and policy management, as well as to establish a growing presence in social networks. These platforms, supposedly, should be aimed at improving interactive processes between public bodies and citizens, facilitating fundamental issues such as transparency and participation[2].

But why should an analysis of information security be carried out for the voting processes of sectional governments in Ecuador, and how safe is the entry of this information (results) into the voting system? To improve the security, integrity and confidentiality of information in the voting process, both at the sectional and national levels, there must be processes, quality standards, computer security policies (PSI), encryption algorithms and information access security, the implementation of

[*] Segundo Moisés Toapanta Toapanta, Email: stoapanta@ups.edu.ec

these processes and policies ensure the management of information in the institution, thus preventing theft of information and manipulation of votes in electoral processes.

The main objective is to analyze the processes, policies and cryptographic means that secure the information and are implemented by the CNE, so that in an electoral process the management of it remains confidential, available and integrated and no third party can adulterate or gain control of it.

The method used in this study uses a qualitative, deductive, descriptive and exploratory research approach to analyze reference articles, Ecuador's articles of law and analyzes carried out in past votes.

Concluding that the processes and policies proposed by the entity are based on the pillars of information security of the ISO 27001 standard, it is also pertinent that the cryptography implemented by the CNE with the hash code is in constant integration with new cryptographic methods. robust and safe to provide greater security, integrity and confidentiality in future electoral processes and avoiding alterations in the data entered in the electoral process.

2. Materials y Methods

2.1. Methods

For this study a qualitative method was applied to analyze the security of the information necessary for an electoral process and that is applied by the CNE. It is also descriptive because the objective of the investigation is to analyze the standards, protocols, encryption means that ensure the information and the external media that attempt against it, and it is exploratory because the different reference articles, of the law of Ecuador and security analysis carried out in previous votes in the country were reviewed. Considering the important aspects of an information security analysis for a sectional voting process in the country.

2.2. Materials

In order to carry out this study, reference articles, articles of law of Ecuador and security analysis carried out in past votes in the country were considered, which provided a contribution to the proposed topic.

The articles of the Constitution of the Republic of Ecuador indicate the duties and rights for the electors, such as Art. 62 which states: “People in political rights have the right to universal, equal, direct, secret and public scrutiny vote”[3].

Electronic voting systems are critical security systems that require early identification of security requirements and controls based on the analysis of possible vulnerabilities, threats, attacks and associated risks[1].

In Ecuador the voting processes are not one hundred percent digital, an electronic voting system is not handled, compared to other Latin American countries such as Venezuela and Brazil, in 2004 the electronic voting pilot was implemented in the provinces of Guayas, Pichincha, Azuay, Imbabura and Manabí. The most recent tests were in 2014 in the provinces of Santo Domingo, Azuay and certain areas of northern Quito, after these tests it was announced that the year 2017 would be implemented nationally, but it could not be since in the year mentioned for the elections it was announced by the CNE the non-use of the same because of its high cost of implementation nationwide.

Knowing this, the voting systems in Ecuador with the issuance of the regulatory framework, the Information Security Officer (OSI) of the CNE, initiated the implementation process, socialization of the PSI (Information Security Policies) within the CNE at the national level, emphasizing that there are two ways of having the information, these are in physical and digital[4].

The use of TIC, security policies, platforms, encryption methods and the knowledge of those involved in the subject make it possible for risks in computer systems to decrease and even prevent malicious accidents that compromise availability, authenticity, integrity and confidentiality of information systems in electoral processes.

Today the security of companies or entities are based on three main fundamentals:

- People.
- Management.
- Information Technology and System.
- Logical Security.

All this information and data that will be entered in the voting systems in an electoral process must be encrypted in cryptographic algorithms in which we can define the following:

- Symmetric algorithms.
- Asymmetrical algorithms.
- Hash Functions.
- Digital Signature and Certificates.

Likewise, the National Electoral Council (CNE), as part of the electoral function of Ecuador, has the responsibility of “Organizing, directing, monitoring and guaranteeing, in a transparent manner, the electoral processes; convene elections, carry out electoral calculations, proclaim the results, and possess the winners of the elections ”(Art. 219 of the Political Constitution)[4].

I) Electoral Process in Ecuador.

The National Electoral Council (CNE) is the institution. that decides the use of electronic voting methods and / or total or partial scrutiny in the different elections in accordance with art.113 of the current democracy code[3].

The electoral process in Ecuador is physical and digital, the physical and manual form is divided into four phases:

- Installation and arrival of voting board members (JRV).
- Voting and receiving the vote.

- Counting and counting of votes.
- Packaging and shipping of material after counting.

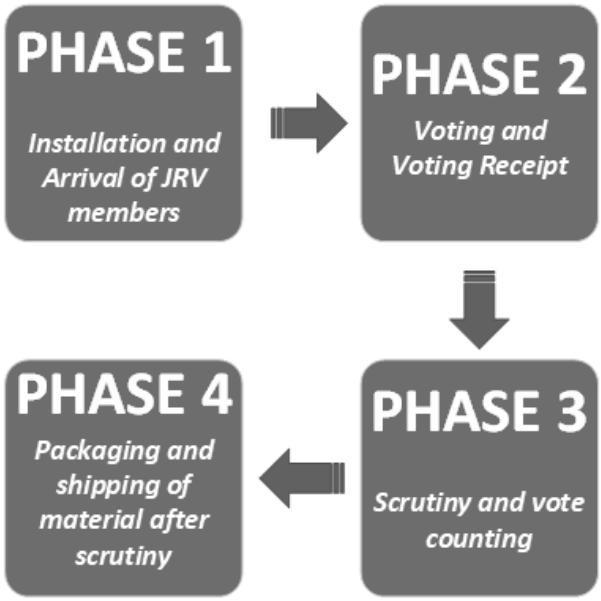

Figure.1 Electoral Process Phases

The processes carried out by the CNE for the 2017 electoral process, evidenced the application of the PSI for the management of physical information, to maintain the integrity of the documents both in manufacturing, transportation, and systematization. Physical information available in the electoral material includes:

- Patrones electorales.
- Installation Minutes.
- Voting Ballots.
- Proceedings of scrutiny among others.

All electoral documents were prepared by the Military Geographic Institute (IGM), as well as the logistics and transportation of electoral material for an electoral process is under the CNE cooperation agreement with the Ministry of National Defense and the Ministry of Interior, where The responsibilities of each Defense institution in an electoral process are clearly indicated. Given these scenarios, it should be taken into account that technological advances are already within the democratic voting of Ecuador, with which the CNE took into account that a filter of primary security of the information to be protected is managed by people, therefore the aspect of trust is a key piece to guarantee the viability of the information entered, therefore the agency must be able to determine neutral personnel for the counting and entry of the information in the system by carrying out security policies according to the information that is handled .

II) Information Security Analysis

For the 2017 electoral process, the CNE, through the National Information Office, developed with its own staff, computer systems that store the digital data of the 2017 electoral process. Among the main systems developed are the Registration of Candidacies, Selection of members of Vote Receiving Boards (MRJV), Scrutiny System, among others[4].

So that the CNE Voting System were not vulnerable to fraud, threats and associated risks, the National Electoral Council developed processes and procedures following the ISO 27001 quality institutional models and PSI procedures that the CNE has approved and among which we have:

- Access Control Policies.
- User creation standards, network computers, servers, database.
- Secure configuration standards for wireless networks.
- Password standards.
- Cryptographic control standards.
- Standards for VPN configuration.
- Third Party Interoperability Standards.
- Computer contingency plans, among others[4].

These procedures were developed according to the main pillars for good information security management as described in figure 2. These are:

- Confidentiality Of Information.
- Integrity Of Information.
- Availability Of information.

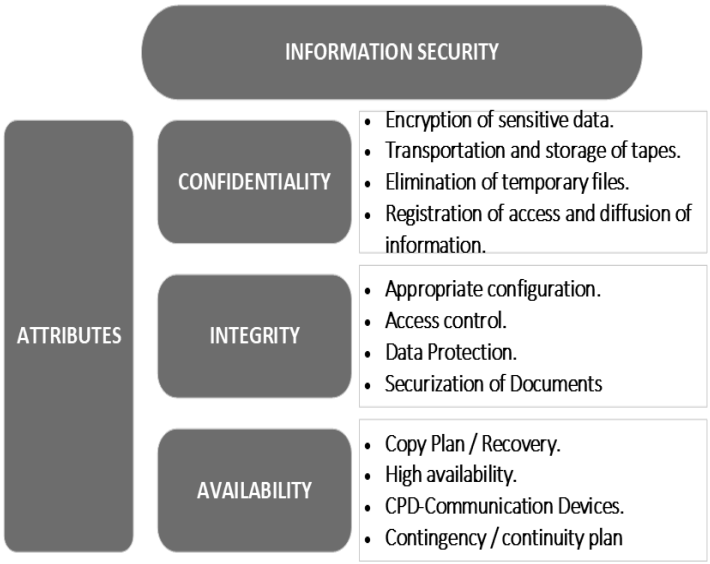

Figure.2Pillars of Information Security[5].

In a voting process, whether physical or digital, it involves the intervention of different entities, such as: voters, vote counters, registration centers, ballots and voting boxes, to name a few[6]. In this way, it is understood that, in the face of so many involved, greater care must be taken of the leak, damage or loss of information. There is also a variety of Information Security services that provide a guarantee that protects the data within the system and everything that is done on it.

According to Tossi, the cyberattacks correspond to denials of service, introduction of viruses, malicious program and/or Trojans that cause loss of information or will prevent normal network service, mail web services, and computer systems. International

evidence shows that the most important attacks are "denial of service" against government networks and private company websites to disrupt or disable their normal operation; to erase or destroy vital information in private or state entities and attacks to degrade or disrupt industrial control systems[7].

The processes of digital voting must be synonymous with integrity, audits, confidentiality and access control, but not during sectional elections, but from before, since an electoral process carries its own demands. That is why information security objectives were established in the election processes in the country.

Table 1: Objetives for Information Security

Objetives For Information Security	
Data Integrity	During and after the election process.
Audit	That can be auditable, at any stage of the process.
Confidentiality	Information integrity and non-denial.
Access Control Policies	Security policies both physical and digital in controlling access to staff of the CNE.

The computer systems linked to the 2017 electoral process were verified by accredited auditors of the political organizations, according to the audit plan that was approved by the Plenary of the CNE (Minutes 14-PLE-CNE-2016). In the observations, different types of assessments of the systems developed by the CNE could be carried out. As an important point, it is mentioned the obtaining of hash codes of the counting system on the day of the election, both in the first and in the second round, in order to have a verification element, both for the CNE and for the organizations policies, where the integrity of the information between the system audited by the political subjects and the one used for scrutiny on election day is evidenced[4].

For the approach of a universal security system according to any type of information system, four approaches can be identified:

- Prevention.
- Detection.
- Forensic.
- Response and Action.

Each of these approaches makes a reference to the role each has in relation to the information system.

There are systems such as the UPS (Integral Administrative System) that was implemented in Venezuela on some occasions, which uses the fingerprint for the electoral process where it is verified that the voter is the corresponding one according to their identification so that the machine is active with the validation of the footprint and the voter's identity card.

For his part, Bast Silva, indicates that in electronic voting systems it is necessary to protect. Indefinitely the visitor's privacy even after the election is over, since in case any intruder obtains a digital copy of records that allow the voter to relate to their vote would have all the time to try to decipher it.

People want to keep their privacy secured indefinitely and there are cases in which it would be of the utmost seriousness to know who a person voted. For example, knowing the trajectory as a voter of a current candidate could influence the electorate.

During the electoral process the data security lasts: the protection of the circulating information should only support the period that corresponds to the voting process[8].

Organizations that wish to establish the self in a globalized and competitive market such as today's should have an infrastructure that allows them to interact with their environment in an appropriate way, facilitating the promotion, dissemination and/or provision of their products or services through such a technology platform. However, the destination of such disclosure, processing and/or information processes are not always directed towards the external scope of the organization, but can and should be implemented into the internal processes of the organization, in order to streamline the channels of process control, information (formal and informal), disclosure of policies and feedback of those nerve elements in the organizational work. Despite all the efforts, Charlemagne, in his studies shows that, despite the new channels and digital media, the basic interaction between representatives and represented is constantly relegated[9].

One of the relevant aspects during and after the voting process, is to save the data, for this Legorreta, points out that the transformations that society has suffered over time have led to the raising of new questions about the way in which many of the processes are carried out within a State[10].

The electoral sphere has not been exempted from these transformations. Being the State, who must ensure that the processes are handled efficiently and responsibly.

According to Del Monte, the use of technological resources during an electoral process involves three specific areas:

- Creation of the voter database.
- Total calculation of votes and total aggregation of votes and transmission of results
- Publication of votes and partial results[11].

While the counts have changed, they have influenced using technology has allowed the creation of new means of voting, where technologies are active participants, their foray being for some years in different countries. Manual counting times now involve the use of technologies for electoral management, although this adds benefits in speed, this implies a high cost, both economically as long-term and socially and politically.

In countries like the United States with regular electoral processes, they have already been introduced with equipment that is used to collect votes and then be counted automatically. For this, laws and a jurisdiction have been created that envisages a very rigid state policy.

According to Morales, in that line, people's adaptation to communication and information technologies has been mediated by the level of internet access and the broadband capacity available to them. Thus, the presence of electoral processes in the virtual space depends not only on the characteristics and transformations of web 1.0 to web 2.0, but also the possibility of internet access[12].

There are in turn protocols that have a universal acceptance at the moment to transmit information or data on the Internet, it aims to effectively transmit the information, in addition, by carrying out automated processes, it will allow to expand its performance so that this is implemented within the technical area under way:

- Reduce investment in raw materials, along with human resources.
- Clarity and certainty in the choice of authorities.
- Create favorable conditions for access to suffrage, through conditions that make it easier for the user to comply with their right safely.
- Process information requirements quickly and efficiently.

In addition, Ávila Barrios points out, So far commented that it can be considered an error to address the issue of Electronic Government (GE) only from a technocratic perspective, since it is about having, through the use of technologies, a platform that allow to successfully implement participatory processes, with efficient and transparent procedures that provide effective services to citizens[13].

The information handled in an electoral process would maintain the use of security processes, with data being that are compromised and vulnerable, can be seen in Table 2.

Table 2: Data that Require Security

	Confidentiality	Integrity	Availability
Electoral Roll	NOT	YES	YES
Votes	YES	YES	YES
Candidates	NOT	YES	YES
Income of result	YES	YES	YES

It is a difficult task, but steps are being taken to improve the electoral system and this requires planning, investment and technological updating, as well as Aguilar, notes that the application of new technologies in electoral matters has increased worldwide in the last years[14].

III) Cryptography in Information Security

Information entered an electoral process is the main and most important element in an electoral process, it is sensitive information that must be protected and protected.

Any new approach that comes up is quickly made available to a huge critical mass that evaluates and generates the changes it deems necessary. Simultaneously, the geometric growth of a cryptanalyst's attack capacity requires a cryptographic system to demonstrate security in an undisputed manner, with rigorous formal mathematical techniques to be applied.

Thus, the author García believes that the same is true in the field of computer security in general and in cryptography. One of the reasons for this phenomenon is the large increase in the volume of information available.

- One of the applications with the highest demands in this electronic sense. The results of a vote define important power relations and the management of important economic resources. It is therefore essential to ensure two key points
- The count must transparently reflect the will of the citizens.
- A voter must be assured that their vote will remain anonymous indefinitely[15].

Cryptography in the scrutiny system is used to protect the data transmitted between the voter and the server to ensure that it is not leaked to a third party[16].

The National Electoral Council, as an important point mentions the obtaining of hash codes, this sense, the Hash cryptographic function, is a mathematical algorithm that transforms any arbitrary block or data entry into a series of alphanumeric illegible characters[4].

The Hash algorithm will ensure the integrity of the information due to a system that prevents the manipulation of the results. The identification mechanisms of the users must also be considered, in relation to entering the system with their password, which prevents malicious third parties from wishing to manipulate the system, even preventing these subjects from reversing any procedure already performed by the user. In addition, you can use the digital signature that adds to the user's security system, using encryption with keys that can only be used by authorized persons.

For the cryptographic systems to work, a protocol is required, which allows to follow the respective steps, which avoids the manipulation of some external entity and which allows the proposed objectives to be achieved. Do not underestimate any level of security, so you must be aware of any weaknesses presented and any steps that are not being met accordingly.

IV) hreats in Information Systems

Voting systems even though they have high security standards, however, they can be breached and present certain threats. Among them are:

- Human Threats.
- Natural Threats.
- Environmental Threats.

In the face of the most common threats, several previous practices could be carried out:

- Preparation of Security Protocols.
- Review of Information Security Standards.
- Creation of a Computer Emergency Response Team (CERT).
- Review of Information Security Risk Management Methodologies.
- Review of annual information security reports.
- Mitigate Distributed Denial of Service (DDoS) attacks on Linux platforms.
- Avoid social engineering attacks like spear phishing, which correspond to malicious emails that take users to fake websites with lots of Malware.

According to Camana, the increase in the volume of information that is computerized in digital databases has grown dramatically in recent years[17].

Documentation about the projects to implement automation in the elections, which aims to counteract human error during the entire electoral process, could also be reviewed.

3. Results

Technological suggestions and security measures will enable better counting in a voting process. Abdala says the adoption of electronic voting may have differential effects on election results by affecting voter turnout[18].

In this way, it should be borne in mind that proper handling of information is indispensable, since, when reaching the wrong hands (it can be altered, stolen, deleted, etc.).

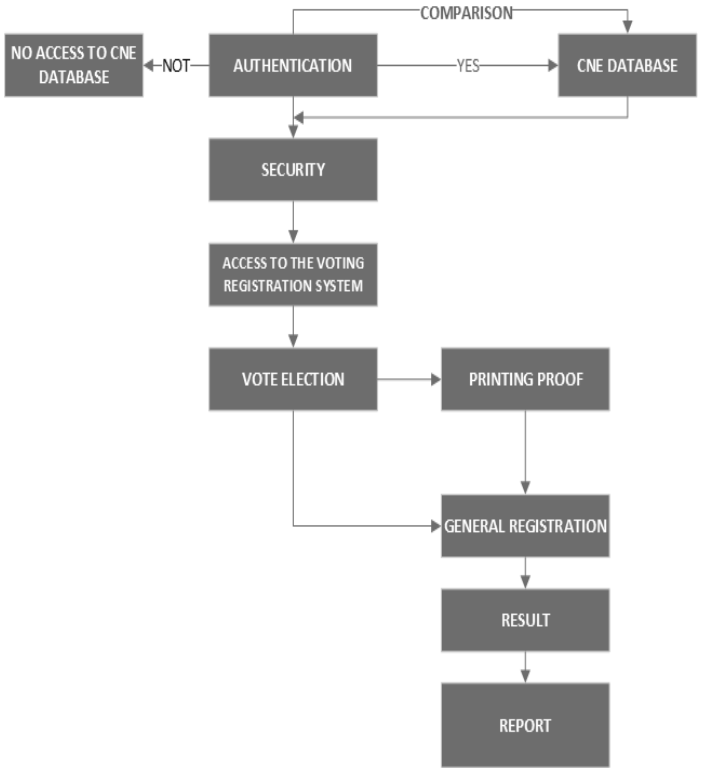

Figure.3 Authentication cryptographic Process

It is also suggested to work with audits to enable it to know whether the mechanism used complies with the security processes and the information entered is being protected and the results are being correct and timely in the voting process, so Rocha, states that, in electronic voting systems, it is extremely important to have a record of events, in order to have the evidence of actions taken especially for cases where manipulations are suspected[19].

- User Authentication.
- Information is encrypted using a cryptographic channel or method.
- If the user complies with security permissions and accesses, the decryption information is verified by security methods.
- If the authentication is successful, the voting registration system is accessed.
- The user casts their vote. Which allows you to print the voting receipt.
- Once the above steps are approved, the general log is generated, its result, and at the end of the report.

It should be added that, the elements that can cause problems to the computer system can be either external (hacker attacks, viruses, espionage) or internal, which can turn out to be very expensive, since, it can be carried out by someone trusted and have direct access to the most important and sensitive information.

Following these considerations, it is possible to avoid computer risks, but also by taking care of possible accidents of nature that may affect processes and through the creation of public policies, establishing rules and procedures that allow safeguard election information.

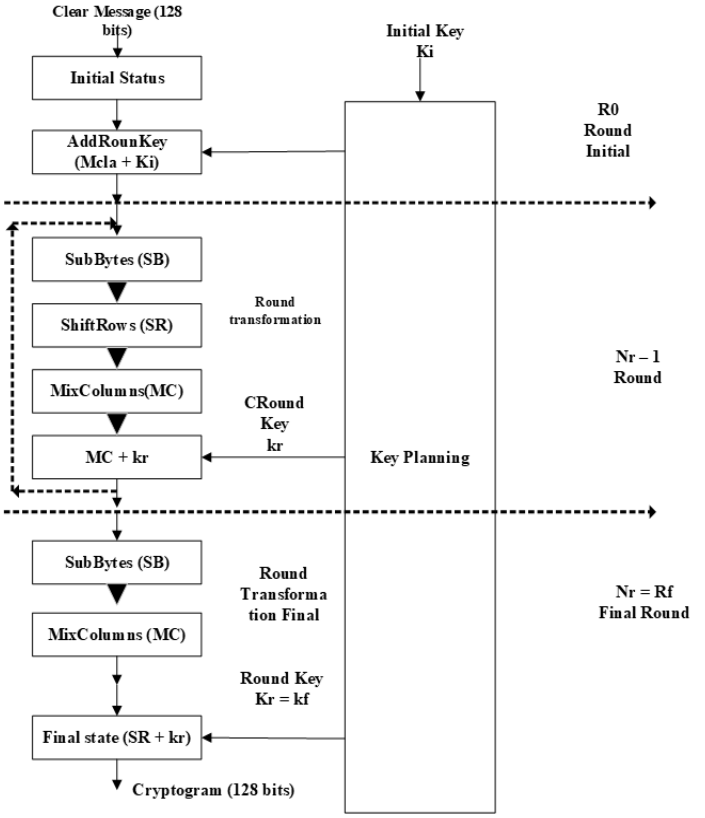

Figure.4 Cryptography AES

It was determined that the combination of the symmetrical system and the asymmetric system can be combined to obtain a better result.

This hybrid security system will prevent external agents from manipulating or affecting the results obtained in the different elections; complementary safety measures have also been analyzed that can help mitigate or avoid possible effects on the results.

The AES encryption algorithms, consists in applying to each state a set of grouped operations that are considered rounds, the algorithm performs eleven rounds, where in each round a different subkey is applied:

- 1 Initial Round.
- 9 Rounds of Transformation.
- 1 Final Round, as seen in the figure 6

4. Discussion

It can be understood that new technologies contribute effectively to progress in each country, in Latino America there are few countries that use electronic voting, Ecuador still does not specify this proposal because of a lack of decision, budget or distrust in political parties. With a good programmed established and following security protocols, its implementation could ensure security, speed and effectiveness, before, during and after the electoral process. Any voting system, whether digital or traditional, will need essential requirements for its implementation. However, there is no voting system that provides this security and integrity of information; more, however, there are aspects that can be taken into consideration to prevent certain attacks.

Hence it is suggested to work with a permanent audit, as noted, Schmidt, the functions of the system should be stored in digital logs that can be extracted later for audit purposes. These blogs can also be used as duplicates of the documents required by current legislation[20].

But it is also suggested to take brief steps to develop an appropriate security system:

- It is necessary to recognize the required infrastructure and the proper security measures both physical and digital, as well as the care of those who have access to such information and the custodians who provide security of the site.
- Study the vulnerabilities that can occur within the system and the enclosure where such data is permanently located, as well as external attacks that attempt or violate security measures.
- Develop a contingency plan in case security measures are breached.
- Have a team of professionals dedicated to maintaining stability and security in networks and identifying potential vulnerabilities, as well as malicious attacks, fixing open door problems.
- Establish security policies both in the use of the system and in the responsibilities in case of eventualities during its application.

Security systems that are applicable in some contexts have been noted that they do not have the same effect on others so models vary in countries that use electronic voting systems in whole or in part, as is the case in Argentina compared to Venezuela, which apply different models. Thus, the suggestions made for Ecuador may be effective if other complementary aspects are met.

Despite the contrary intentions, from some malicious and direct sources to the electoral system, these suggestions will mitigate external interventions that want to change the election results.

5. Conclusions and Future Works

5.1. Future Works

Design of security protocols, new cryptographic methods and effective physical and logical security measures to prevent information leakage and modification of the results obtained in the different votes, thus avoiding problems with the information entered in the electoral process.

Strategies for the protection of precincts before, during and after sectional voting, using advanced technology.

Technology security audit, which allows monitoring the compliance of the phases during the electoral processes.

5.2. Conclusions

In the voting processes for Sectional Governments in Ecuador and requires working with a design of security protocols with strategies that counter social engineering attacks by preventing the leakage of information and modification of the results obtained in the votes.

It is necessary to use new technologies so that the results obtained are reliable, it is pertinent that the cryptography implemented by the CNE with the hash code is in constant integration with new more robust and secure cryptographic methods to maintain an adequate security standard, since it allows a correct encryption of the information, providing greater security, integrity and confidentiality to the corresponding votes, likewise care must be taken of content uploaded in clouds or on state government platforms, because they can be vulnerable to specific attacks by malicious codes or by denial of service.

Finally, to involve international entities which allow audits to be carried out and help improve the current state of information security systems in the country.

Acknowledgment

The authors thank the University Politécnica Salesiana of the Ecuador, to the research group of the headquarters of Guayaquil "Computing, security and Informatics for a globalized world" (CSITGW) created in accordance with resolution 142-06-2017-07-19 and the Secretariat education higher science, technology and innovation (Senescyt).

References

[1] C. D. De Faveri, A. Moreira, J. Araújo, and V. Amaral, “Towards security modeling of E-voting systems,” Proc. - 2016 IEEE 24th Int. Requir. Eng. Conf. Work. REW 2016, pp. 145–154, 2017.

[2] J. Rojas-mora, "Desafíos jurídico-políticos en el entorno digital Sulan Wong Ramírez Julio Rojas-Mora Helder Binimelis Espinoza," vol. 28, no. 2015, pp. 8–12, 2018.
[3] A. del Ecuador, "Constitución del ecuador," 2008.
[4] J. Badí and Q. Basantes, "Análisis de la seguridad integral en los procesos electorales : Caso proceso electoral 2017 de Ecuador," pp. 105–130, 2017.
[5] Telefonica, Ciberseguridad , la protección de la información en un mundo digital. Madrid, España: 2016, 2016.
[6] G. Gallegos-garcía, R. Gómez-cárdenas, and G. Duchén-, "Protocolo de votación electrónica basado en emparejamientos bilineales Electronic voting protocol from bilinear pairings," pp. 234–244, 2010.
[7] A. A. TOSSI, "Revista Política y Estrategia," vol. 125, 2015.
[8] S. Bast, P. García, and G. Montejano, "OTP-Vote : Avances en la Generación de un Modelo de Voto Electrónico," pp. 1069–1073.
[9] M. C. Carlomagno, S. S. Braga, and R. C. Sampaio, Respondem os políticos a questionamentos dos eleitores ? Um experimento controlando os incentivos de mensagem , período e meio, vol. 24. 2018.
[10] P. Carolina, G. Legorreta, P. Carolina, and G. Legorreta, "Voting from Abroad: What Did We Learn From the 2006 Experience?," 2014.
[11] F. B. del Monte, Límites y potencialidades del Voto Electrónico. 2007.
[12] J. A. Morales and J. Alexander, "El impacto de la interacción virtual en los procesos electorales en México," vol. 9, pp. 9–45.
[13] D. A. Barrios, "La implementación de Tecnologías de la Información y Comunicación (TIC) desde finales del siglo pasado produjo , a escala mundial , importantes cambios en todo ámbito , sea privado o público , desde la forma de organización personal e institucional hast," 2014.
[14] D. E. Aguascalientes, A. Lilia, S. Aguilar, C. Gutiérrez, L. Cristina, and P. Howlet, "Electronic voting : reliability and implementation of technology," pp. 77–83, 2017.
[15] P. García, G. Montejano, and S. Bast, "Seguridad Incondicional para el Anonimato en Sistemas de e-Voting," 2015.
[16] L. Rura, B. Issac, and M. K. Haldar, "Secure electronic voting system based on image steganography," 2011 IEEE Conf. Open Syst., pp. 80–85, 2011.
[17] R. Camana, "Potenciales Aplicaciones de la Minería de Datos en Ecuador Minería de datos : Orígenes y Conceptos," vol. 29, no. Julio, pp. 170–183, 2016.
[18] M. Belén, A. Benesch, and A. Pedro, "Evaluación de los efectos de la Boleta Única Electrónica : evidencia experimental de las elecciones en Chaco 2015 * Evaluation of the effects of e-voting : Experimental evidence," 2016.
[19] L. Felipe and F. Martínez, "Audit Mechanism for Detecting Voting Manipulation in Electronic Voting Systems Audit Mechanism for Detecting Voting Manipulation in Electronic Voting Systems Óscar Ruiz Hernández **," no. January 2018, 2019.
[20] J. Hacia, "Hacia el desarrollo de un prototipo de sistema de voto electrónico para Costa Rica Towards the development of a electronic voting system prototype for the Costa Rican context," vol. 29, pp. 146–158, 2016.