ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 5, 53-60 (2019)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Proposal for a Security Model for a Popular Voting System Process in Latin America

Segundo Moisés Toapanta Toapanta [*,1], Allan Fabricio German Diaz[1], Darío Fernando Huilcapi Subia[1], Luis Enrique Mafla Gallegos[2]

[1]*Department of Computer Science, Salesian Polytechnic University (UPS), Guayaquil, Ecuador*

[2]*Faculty of Systems Engineering, National Polytechnic School of Ecuador (EPN), Quito, Ecuador*

ARTICLE INFO

Article history:
Received: 08 July, 2019
Accepted: 21 August, 2019
Online: 03 September, 2019

Keywords:
Technology
Electronic Vote
Electronic Security
Technological systems
Individual reinsurance

ABSTRACT

In Latin America, there is a need for better security systems in different national or sectional votes, which is why this study was carried out, to show a proposal for a security model that helps to obtain better results and to this purpose has been selected information on the database for different Latin American countries, it has also been considered descriptive aspects and with a quantitative approach, to provide an objective livelihood. It has been intended to identify several security requirements that give confidence to citizens. Currently in Latin America studies continue to be carried out on technological systems for electronic voting and their real effectiveness in different countries, and then improve or implement them. Not all have come to implement it completely but in part due precisely to the demands it demands, also because of the limited information and because there are few related studies on these issues. The growth of technology and its easy access has allowed it to be used in different areas and politics is no exception, which is why different modalities of electronic voting have been implemented so that they can reduce some failures that are maintained in the traditional voting system. In conclusion, it is noted that voters need to know better about the new systems applicable to counting, it encourages individual reinsurance, which does not reveal the identity of the voter, as well as transparency, easy access information and auditability. Awareness is suggested about the use of electronic voting and the benefits it brings without also excluding negative factors because there is not totally secure and reliable digital voting system. Citizen participation must go hand in hand with political decision-making, so that processes are transparent, and results are protected. With all these criteria it can be noted that it is necessary to consider a comprehensive electronic security model that guarantees that reliability and integrity of the secret election vote, bearing in mind that the purpose is to reduce and prevent errors.

1. Introduction

Several Latin American countries are implementing new technologies and wish to implement it in the electoral system through electronic voting. Few countries are already using it with relative success, as each electoral process receives serious criticism, even in Venezuela the results achieved in the last elections have been rejected. These events require a thorough analysis, to know if the process has been inconvenient or the problem has been in pre-election events, which have nothing to do with existing technology platforms.

Author Diaz Ricardo refers that the momentous changes in the modern world, characterized by its interesting development, the accelerated globalization of the economy, the sharp dependence that incorporates a high volume of information and the systems that provide it; the increase in vulnerability and the broad spectrum of threats impose new challenges on the practice of the audit profession, in particular to the computer security audit [1].

The use of ICTs in Latin America has been increasing and it has been desired to be applied in electronic voting to generate an effective and transparent information process. E-voting or electronic network voting is an applicable mode via the Internet, as well as the electronic ballot box that has the most acceptance and use in Latin America compared to the other existing modalities.

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

If we are thinking of implementing a security system, it is necessary to establish the voting mechanism that best meets the requirements of each country, as well as to think about the scopes and budgets that are needed for its applicability. The author Muñoz points out that organizations need a stability and greater degree of protection focused on computer security to protect and minimize threats to their information [2].

Considering the benefits and potential expenses make the decision more difficult to make, as well as having people who handle these systems with the greatest care that these processes deserve, so the challenge of using technological aspects requires that citizens and the authorities in charge maintain ethical criteria to avoid the different types of fraud that may change the results obtained. Process management and the application of security systems will make security systems applicable to each Latin American country, under any type of government.

2. Materials and Methods

2.1. Materials

The material used has been selected based on data relating to different Latin American countries, among these, articles based on the implementation of different modalities of electronic system and the benefits it provides. Current work was also considered to make security models applied to electoral systems relevant.

The information has been relevant and closely related to the subject matter of this study, to consider the urgency of presenting a security system in the voting system of Latin American countries. Several Latin American countries have seen suffrage security measures applied in other countries in the region, while the will to implement electronic voting is being considered, including Argentina, Chile, Peru, Uruguay and Costa Rica.

In the region only Brazil and Venezuela show the use of electronic voting, but that as in any electoral system, there are reports of the results obtained. According to Hosp and Vora's theorem, there is no electoral system with perfect integrity, verifiability and privacy, as malicious attempts to modify the results will always be found.

But you can count on important suggestions such as individual reinsurance, which does not reveal the identity of the voter, as well as transparency, with easily accessible information and auditability, that allows access to the result obtained, appropriate use of technological equipment that does not keep a voter's record, the key safeguarding, which in the case of using cryptography, must specify how and who will be responsible and also restrict access to the different equipment used.

2.2. Methods

This work has a quantitative approach since information is presented in an objective, graphical way and making use of available resources. It also considers inductive, deductive and correctional aspects, with descriptive criteria of the process to be followed in the proposed safety system.

For this reason, the studies carried out in this topic are valued, in relation to technological resources, since they are being used in different areas that demand their immediate application.

I) Electoral Information and Technological Modernization

Technological innovation has a great impact and acceptance worldwide especially in Latin America. This implementation in the different countries has provided several benefits in the different processes that make use of technological means.

The author Curious to make most of the benefits of technology, the State requires an appropriate physical infrastructure that supports it through a large transport and access network that allows it to integrate into other networks [3].

So also, the author Jerez points out that the contemporary discussion on public spheres has been expanding the focus of analysis focused on social and political actors towards that of institutional and cultural regulations in public spaces and as key areas of production of ideologies, identities and agendas. To a large extent on these discursive plots, the social conflict and institutional dialogue that processes collective problems is deployed, demeaning which will be defined as public and private interests to be addressed (or not) by each State in a context national history given [4].

In the public and private spheres, they require the development of appropriate technologies, because of the easy access to the information they provide and in addition to their easy management, taking into account that ICTs have also reached each person through the mobile phones, the internet, among others, in such a way that their use is daily and the connection with the different processes of each organization keeps them close.

For his part the author Rovelli, several countries in Latin America were the scene in the last 15 years of intense socio-political and techno-economic changes driven from different policy trends, which converged in principle and to the less from a normative level in a greater presence of the State in the social sphere and the search for alternative and innovative ways for development [5].

Technological innovation, as well as taking part in different organizations in which they provide services such as health, education, entertainment, etc., has become part of the political processes of each country, as in the voting system via Electronic. This has benefits, but there are also risks. An example of electronic security problems occurred in the USA, so author Ottoboni refers that the State of Georgia was a focal point in the civil rights movement of the twentieth century. also has a history of electoral problems: suppression systematic voter voting machines that are vulnerable to undetectable security breaches, and serious security breaches of their data systems [6].

Likewise, in addition to the agility provided by electronic voting, transparency is needed throughout the process, as there are factors that can have a direct or indirect impact during the process or on the use of information.

That is why it is essential to have a security model that is applied in each electoral process in such a way that it can be replicated in other Latin American countries. These technological means also seek to prevent any act of corruption that alters results in such a way that the level of transparency in electoral processes is evident to all voters.

The use of ICTs in electronic voting is intended to generate an effective and transparent information process, which is why there are currently many modalities that are in line with this. A good development of the electoral process through the automation of the vote will also depend on the security model that it uses in order to achieve a correct and adequate management of the information, whatever the mode of the vote to be used.

The different governments of Latin America have decided to implement the automation of the electoral process in order to reduce time, space, resources, among other aspects; considering also the benefits it provides and the great changes it has brought through its use in such a way that citizen participation increases and the voting system is easy and accessible to all.

Like any electronic voting system, they must rely, in dispensing with, security requirements that give voters confidence, make good use of stored information, take care of personal data, and keep the right to integrity of the voter and their decision on the vote.

Studies on electronic voting systems and their real effectiveness in different countries are still being carried out. Not everyone has come to implement it completely but partially because of the lack of security it has in terms of it because of its limited information and related studies on them.

Little information that needs to be reduced in society in such a way as to raise awareness of the use of electronic voting and the benefits it brings without also excluding negative factors because there is no totally secure digital voting system and reliable.

II) Electronic Voting Modalities

Thanks to the technological modernization to which the world has become, mechanisms applied to the electoral field have been observed, with multiple systems that provide what is expected in an electronic voting system: Trust, security, among other characteristics, that a system must rely on, in addition to reducing the costs of the required election materials.

Author Mellinghoff believes that when voting there must be the principle that elections should be secret, it ensures that the voter is the only one who knows the content of his election decision.

This principle is the most important industrial protection for freedom of choice. It obliges the legislator to take the necessary measures to protect the secret ballot (e.g. covered ballot, booths that guarantee voter privacy).

Any investigation of voting intentions or voting of voters is prohibited. Any exception to the secret ballot is permitted only if it favours the right to vote, that is, in cases where the principle of general and equal elections requires a procedure in which it cannot be guaranteed in each case that the vote is absolutely secret [7].

However, it is considered that these are not exempt from any error or failure situation due to some factors to which they may be vulnerable and become a threat thus causing the alteration and loss of information.

According to the author Schmidt, it refers that, in its broadest form, electronic voting refers to the use of electronic technology for the automation of an electoral process [8]. But not just any technological system, but that which applies to the Ecuadorian context.

The author Sandoval indicates that theoretically electronic voting on the internet can be considered a more form of e-vote, so it can be considered that there were some precedents in this regard [9].

There are two types of electronic voting:

- Remote electronic voting.

  Emission of votes through any device (computer, mobile phone, PDA, etc.) with internet connection.

- Electronic voting in person.

  Issuance of Votes from electronic voting terminals from the polling stations (JRV).

It is necessary to emphasize that there are several models of electronic voting in person, among which the electronic ballot boxes stand out, these are carried out in person, that is, located in each electoral roll.

The e – electronic voting or electronic network voting is done via the internet; the reading is automated and can be seen in Figure 1 below.

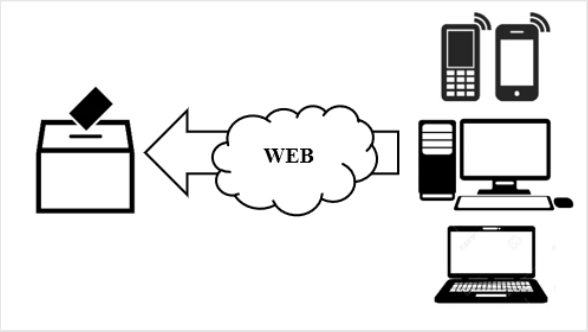

Figure 1: Electronic Vote Models

The electronic urn has the greatest acceptance and use in Latin America compared to other existing modalities; it is carried out in person where there are authorities responsible for the surveillance and control of the votes, in the ballot box for their proper management and organization.

On the other hand, when using digital instruments or technological equipment to represent the use of ballot boxes, it is considered the introduction of elements that are similar in their application but that allow the management of information in a safe, transparent, fast and practical.

For the vote to be served, electronic ballot boxes and the internet are required at the polling place, as shown in Figure 2.

These machines automatically identify the votes where the count is made after this and then be sent to a center that collects all the votes obtained from the polls throughout the country or city and finally obtain the final result of the electoral process.

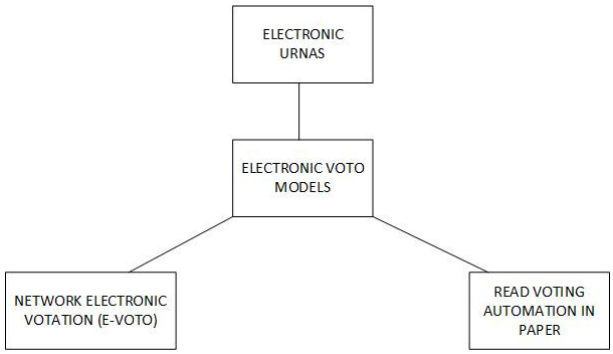

Figure 2: Main Mode Used

Author Abdala indicates that empirical evidence on the extent to which different voting technologies affect election results is far from conclusive. However, irrespective of the causal mechanism used to explain the results, there is a kind of consensus on the importance of the voting system. It is necessary to understand how voting technologies interact with citizens to model political behavior [10].

Electronic voting systems have their advantages and benefits aimed at an entire society not only because of its easy and convenient access or handling, but also because this system avoids long hours of waiting to meet the candidates elected by the majority of s as this speeds up the process by automatically and immediately counting votes.

Among the advantages of using electronic voting we have the following presented in Figure 3.

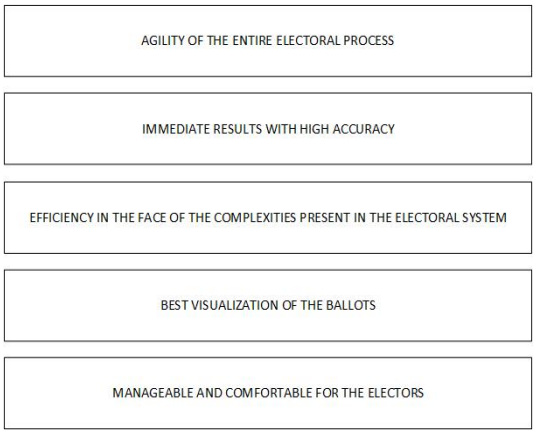

Figure 3. Advantages of using Electronic Vote

III) Electronic Vote Controversy

Despite the many benefits of the electronic voting system, doubts remain around it, in some parts of the world.

Many of these doubts arise due to the lack of knowledge that the company still has in relation to the functions of the electronic voting system, its use, access, among others. Another doubt that society maintains is above all what is related to the security of the system, that is, whether the system effectively keeps the vote, maintaining its integrity, showing no kind of relationship between the vote and its voters.

A. Possibility of System Infringement

Electronic voting systems have a number of measures to regulate or reduce vulnerabilities in the use of these software. Author Lagunez notes that political activity on the Internet is not just marketing, nor social mobilizations; governments have been violated over the Internet by hacker groups called cyber-activists, ideological groups operating over the network. the political activity of these groups goes beyond symbolic protest, they are able to infiltrate the official pages of governments and political, religious and even criminal groups. The space of political struggle becomes more significant because it is shown that the state does not have complete control of a space that can be used by many people; although it is important to remember that it is not yet a totally global phenomenon [11].

Therefore, this modality cannot be considered very reliable either. On the other hand, even if it does not hurt to consider some points that in some way or another can help them not happen so often and do not cause any alterations.

The author Castillejos Lopez indicates that addressing the issue of security in digital environments invites us to reflect on the benefits of using the internet in 21st century society. [12]. The author Bolañoz Burgos points out that while Ecuador defines computer law as the set of legal systems established in order to regulate the processing of information [13].

These vulnerabilities can occur at any time, in an unforeseen way in such a way that the information that is stored can be manipulated and in turn disclosed which could have various negative consequences, in addition to alter the results of these elections.

B. Actors Who Can Break the System

These vulnerabilities are commonly presented by third parties, either with some malice for committing fraud or other evil, nor is it ruled out the fact that this can happen due to ignorance of it and therefore has not been Intentional. The author García, says that security in computer networks will always be a relevant and of interest topic at the computer level [14]. So also the author Castillo points out that precisely because of the different vulnerabilities that exist is that not all countries implement those electronic voting systems for fear of their alteration or fraud that may exist, even because of this uncertainty if your data and your choice will be secure and alter your integrity [15]. This weakness is latent and can affect the security, integrity, availability of sensitive information these systems handle.

In this way, it will be taken into account that these failures do not always arise specifically by electronic voting as such, but that there may be multiple causes such as in the architecture of the system in such a way that it may cause some alteration of the votes made.

Author Avila mentions the campaign season providing voters with a complex information environment in their search for information to guide their vote. These vulnerabilities can become threats to the good performance of electronic voting systems, as environmental and natural threats in addition to the human threats already discussed above. These threats can affect the electoral process and alter the results. Many of these vulnerabilities and threats are uncontrollable by humans as they can happen

spontaneously, however, certain situations can be prevented. The author Lavin José points out that, once these tools and technology have been examined, it can be said that there is a good electronic basis for establishing a Model of Deliberative Democracy since we not only have tools that would allow the vote, but also also the debate, reflection and weighting of opinions [17].

C. Suggestions for Decreasing System Infringement

It is vitally important that society's opinion on the implementation of new voting arrangements is reported and considered as all citizens must feel confident in the electoral process so that this does not then influence the decision of their vote. Keeping voters informed will reduce vulnerabilities to the system, as everyone will cooperate with the care of their votes and follow protocols in every part of the electoral process.

So citizen participation must be a constant reality, in this way it can be said that it has been worked democratically, then each voter will be able to have the pleasure of accessing their right to vote according to the candidate who meets their expectations, because is a manager of the electoral achievements of your city or country.

Thus, the author Marquez argues that the electoral behaviour of the citizen is based on the calculation of the expected usefulness made by the voter, taking into account the proposals presented at the particular juncture, weighing the costs and benefits of each [18].

IV) Information Systems Security

A. Cryptography

One of the recommendations in the application of electronic voting is the use of Public Key Cryptography Encryption, as expressed by author Marin Bermudez, In the context of telematicvoting systems, public key cryptography is often used to encrypt the vote, so that only the holder of the private key can access and account for it:

- In the previous phase of preparing the vote, the key pair is generated; public and private.
- The public key is distributed to all voters to encrypt their vote with it.
- The private key is kept by the board or electoral committee. Generally this key is chopped and distributed among the members, so that a single member cannot access to decipher the votes.

Once voting is complete, members of the electoral board or committee enter the private key so that they can decipher the votes and recount. This ensures access to voting data [19]. Once voting is complete, members of the electoral board or committee enter the private key so that they can decipher the votes and recount. This ensures access to voting data [19].

A. Event Log

Public institutions are also concerned with the need to introduce other security measures into electoral processes, as author Vera Victor says that there are companies that do not care about implementing computer security measures or if they do they only consider externalities and do not take into account the risks that may arise within them [20].

The author Morales points out 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 manipulation is suspected. in a voting session, for example, you can generate the registration of voter authentication, the event of the selection of candidates, the closure of the session, etc. [21].

B. Preventive Security

Any media or information system must have security requirements and actions to be taken in the presence of a vulnerability or threat. To this end, the following aspects are proposed:

- Prevention of security attacks, which refer to the actions that will be carried out if there is any violation of the information.
- Security mechanisms, which refer to the actions that will be carried out in order to identify, prevent and block any attempt to attack stored information.
- Security services, these refer to the service provided to the person when storing their data and other information.

C. Voting Subject Check

Several electoral contests have shown in the list of voters to citizens who cannot exercise their right to vote, because they have died or there have been candidates in two ballot boxes, which can affect the results, therefore, a secure system is advisable, which it would involve the on-site verification of biometric data, for example, the finding of fingerprints by scanning them to confront those registered at the time of entry to the register, or the iris record of the subject who shows up to vote. This voter check would lessen attacks by hackers who want to use these non-existent voters and turn them into real votes. The author Del Blanco points out that the growing proliferation of attacks makes proper system maintenance crucial. On the other hand, no one can predict long-term computational capabilities [22].

D. Voting Subject Check

For the voting system to achieve its objectives, honest participation of political parties and government is needed, as democracy must be embodied in concrete actions that candidates must respect and maintain. This is the opinion of author Lopez that, in this way, political efficiency would be a neutral element that would call for a vote, but which is earlier or higher than mere voter participation, which is precisely what interests us [23]. To maintain a secure voting system, it is necessary to incorporate certain requirements into work, according to the author Valencia indicates that democracy in the 21st century cannot be limited to the right to vote and be elected. The complexity of our societies and the existence of a plurality of legitimate interests make it necessary to expand the spaces of participation and control in the various entities of the State [24]. On the other hand, the legal framework will allow to sustain every decision that is made around the elections within the country, as mentioned by the author Montalván Calderón, which it is also important to establish certain

guidelines that help to meet legal requirements that have electronic security, these encompass various procedures, transparency, verification and reliability [25].

3. Results

Several results could be achieved in this study:

- Security Analysis in electoral systems in Latin America, according to Hosp and Vora's theorem, is vulnerable and requires greater security measures.
- Suggestions to follow in electoral security systems, with the respective applicability in electronic voting.

In addition, for greater security in the process, a probabilistic model of passwords is chosen: A probabilistic model of passwords is determined by any function P, defined in the space of possible passwords (S) in the range [0.1], which assigns a P(s) to each password in such a way that:

- P(s) ≥ 0, for all password $S\ e^{S}$
- Σ

These models are a critical tool for investigating password security. the definition and interpretation of P(s), depends on the model. The existence of alphanumeric password databases available on the Internet has allowed experimental capture of its characteristics, which are used for the definition of P(s), Markov strings and context-free grammars have been the two models most used to quantify by (P) the probability that password s will be selected, by the user, in the registration phase. These P(8) values are the basis for dictionary attacks and some password security assessment metrics [26].

So also, when we mention the Encryption System, we have El Gamal. Originally ElGamal has the multiplicative homomorphic property, but for the vote count a slight variant is used that is additive homomorphic and that is the one that allows the sum of encrypted votes:

Be a G-switched group of order |G| = q. The public key is (G, q, g, h), being "g" a generator of G, $h = g^{x}$,. "x" it's the private key.

Sea in the encryption of a vote v

$$E(v) = (\alpha, ß) = (g^{r}, p^{v}, h^{r})$$

Being "r" a random value $r \in \{0,1, \ldots, q - 1\}$ and "p" another G generator independent of g.

For two votes v_1 and v_2 encrypted such as:

$$E(v_1) = (\alpha_1, ß_1) = (g^{r1}, p^{v1}, h^{r1})$$

$$E(v_2) = (\alpha_2, ß_2) = (g^{r2}, p^{v2}, h^{r2})$$

The additive homomorphic property is:

$$E(v_1) \cdot E(v_2) \cdot (\alpha_1, ß_1) \cdot (\alpha_2, ß_2) = (g^{r1}, p^{v1}, h^{r1}) \cdot (g^{r2}, p^{v2}, h^{r2})$$

$$= (g^{r1+r2}, p^{v1+v2}, h^{r1+r2}) = E(v_1 + v_2)$$

Among the advantages of VER systems that use EEH are: when operating on encrypted votes you do not need an anonymous channel (unlike the blind signature scheme), the counting process is very efficient since you don't have to decrypt the votes one by one before counting and you don't have to wait for the polls to start the polls to begin counting [27].

A. *Security Analysis in electoral systems in Latin America, according to Hosp and Vora's theorem, is vulnerable and requires greater security measures.*

According to Hosp and Vora's theorem, there is no electoral system with perfect integrity, verifiability and privacy, as malicious attempts to modify the results will always be found. But you can count on important suggestions such as individual reinsurance, which does not allow to reveal the identity of the voter, as well as transparency, that allows access to the result obtained, the appropriate use of technological equipment that does not store voter registration and also restrict access to the different equipment used.

B. *There are different ways of violating the system, internally and externally, for which they need to be identified and followed by suggestions from the team responsible for electoral protection. Suggestions to follow in electoral security systems, with the respective applicability in electronic voting.*

Several Latin American countries have implemented security measures and considered the security measures that are applied in the votes of other countries in the region, while the will to implement electronic voting is being considered, including Argentina, Chile, Peru, Uruguay and Costa Rica. In the region only Brazil and Venezuela show the use of electronic voting, but that, as in any electoral system, there are reports of the results obtained. To pre-caution voting in a country, using new technologies, they should consider one of the three options being used: automated reading of paper voting, autonomous electronic voting and networked electronic voting.

Hence to take relevant security measures, such as preventive security that takes care of the whole process, cryptography, with access keys, the log of events that allows to audit each step, before, during and at the end of the respective vote, the vote and all this in an environment that has been cared for under specific law articulations, in which citizens have participated, as well as political parties.

Hence, it is suggested to work on whatever is necessary, as figure 4 points out, which motivates intervention in all the spaces relevant to the electoral contest.

4. Discussion

Implementing a security model is an important requirement for the use of an electronic voting system, as has been emphasized above, since any electronic system in itself does not provide 100 percent security and because every process is finds susceptible to vulnerabilities and threats that can be raised at any time.

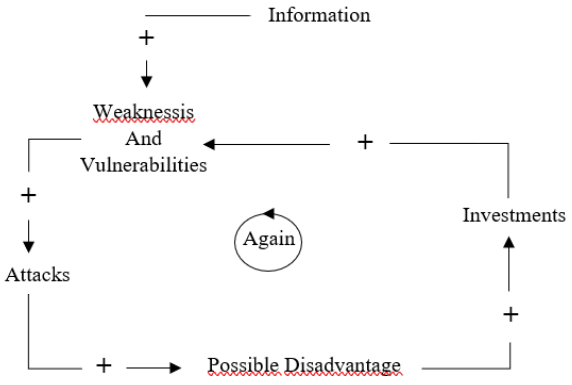

Figure 4: Process to care for a vulnerable system

Any attack on the electoral system will make an impact, but it is possible to reduce it to maximum expression, so you have to be prepared to attack them as soon as they are identified. It is therefore imperative to train staff so that they can follow technical suggestions as needed. In addition, to complement this good management and development of the electronic voting system, it is important to consider that society needs to know the system to be used, its benefits and use. This should be affordable to everyone and must ensure the trust of each of them.

5. Future Work and Conclusions

A. Future Works

- Electronic voting systems with their respective security, for voters who cannot mobilize to their polling station.

- Design of protocols and processes with latest technological tools, for public institutions that control voting in the country.

B. Conclusions

The growth of technology and its easy access has allowed it to be used in different areas and politics is no exception, which is why different modalities of electronic voting have been implemented so that they can reduce some failures that are maintained in the traditional voting system. Some Latin American countries have already implemented and others want to implement several of these models, but in turn it is important to consider a security model that ensures that reliability and integrity of the secret election vote, bearing in mind that it is not equally guarantees its total security, but it does a way to reduce and prevent certain failures.

Latin America suffers from corruption problems and popular voting is always threatened by subjects who wish to change the results, so that the more security options exist during the protocol, the more optimal results can be obtained.

Therefore, it is important to work with security measures that take care of the decision of each voter, such as preventive security, cryptography, auditing, together with the articulated law that are stipulated in the country.

Acknowledgements

The authors thank the Salesian Polytechnic University of Ecuador, the research group of the Guayaquil Headquarters "Information Technology, Security and Information for a Globalized World" (CSITGW) created in accordance with resolution 142-06-2017-07-19 and the Secretariat of Higher Education Science, Technology and Innovation (Senescyt).

References

[1] Diaz-Ricardo, Yanet; Perez-Del Cerro, Yunetsi; Proenza-Pupo, Dayami. System for the Management of Computer Security Information at the University of Medical Sciences of Holguin. Holguin Sciences, 2014, vol. 20, no. 2, p. 1-14.

[2] Mube, Mirna, Rivas, Lizbeth. Current status of computer security incident response teams. RISTI-Iberian Journal of Informacao Systems and Technologies. 2016, No. SPE3, p. 1-15.

[3] Curious, Walter H.; Espinoza-Portilla, Elizabeth. Conceptual framework for strengthening health information systems in Peru. Peruvian Journal of Experimental Medicine and Public Health, 2015, vol. 32, p. 335-342.

[4] Jerez, Ariel; Maceiras, Sergio D'antonio; Maestu, Enrique. Public spheres, political crises and the internet; Podemos's electoral emergence. History, Science, Saúde-Manguinhos, 2015, vol. p. 1573-1596.

[5] Rovelli, Laura-Ines. Recent expansion of prioritization policy in scientific research of public universities in Argentina. Ibero-American Journal of Higher Education, 2017, vol. 8, no. 22, p. 103-121.

[6] Ottoboni, Kelly; Stark, Philip. Election INtegrity and Electronic Voting machines in 2018 georgia, USA, E-Vote-ID 2019 Proceedings, 2019.

[7] Mellinghoff, Rudoff. The German electoral system: overview and new trends. Journal of Electoral Law, 2014, no. 17. p. 1.

[8] Schimidt, Jeff, Alfaro, Jaime Gutierrez. Towards the development of a prototype electronic voting system for Costa Rica. Technology in Progress, 2016, vol. 29, No. 3, p. 146-158.

[9] Sandoval Ballesteros, Netzai. jurisprudential admission of internet voting for foreign residents of Mexico City. Mexican Bulletin of Comparative Law, 2015, vol. 48. 142, p. 275-312.

[10] Abdala, Mary Bethlehem; BENESCH, Pedro A. Antenicci. Evaluation of the effects of the Single Electronic Ballot: experimental evidence of the elections in Chaco 20156. SAAP Magazine. Publication of Political Science of the Society. Argentina political analysis, 2016. vol. 10, No. 2, p. 339-354.

[11] Lagunez Lopez, Oscar Nicasio. for effective democracy: X-ray of a stagnant political system, 1977-2012. Region and Society, 2014, vol. 26, No 59, 9,293-301.

[12] Castillejos Lopez, Berenice, Carlos Arturo Torres Gastelú, and Agustín Lagunes Domínguez. "Security in the digital skills of millennials." Opening (Guadalajara, Jal) 8.2 (2016): 54-69.

[13] Bolaños-Burgos, Francisco; Gomez-Giacoman, Christopher. Qualitative study of the relationship of laws and computer expertise in Ecuador. Receives. Electronic Journal of Computing, Computing, Biometrics and Electronics, 2015, No. 3.

[14] Garcia, Paulo Gaona; MARON, Carlos Montenegro; VELANDIA, Julio Baron. Ontological model for predicting computer attacks from virtualized Honeynets. Logos, Science & Technology Magazine, 2016, vol. 8, No. 1, p. 101-114.

[15] Castillo, Jessica Nataly, et al. Model for reducing it security risks in web services. Summits, 2018, vol. 4, No. 2, p. 19-30.

[16] Avila, Caroline; Cabrera, Gabriela. the effect of the rumor on the change in voting: the anger, fear and uncertainty generated by the rumor in electoral processes and its contributions to voter decisions. Sign and Thought, 2016, vol. 35, no. 69, p. 100-116.

[17] Lacon, José M.; Alvarez, Edison; MAJOR, Franklin. Deliberation and participation: electronic trails. meth. social sciences magazine. 2014, vol. 2 No. 2.

[18] Marquez, Stefany Arteaga. How does the political brain work? guide to political communication to understand voters and public opinion. Mario Alario D'Filippo Magazine. 2018, vol. 10, no. 10, p. 187-212.

[19] Maron Bermudez, Antonio. Study of the use of blockchain protocols in electronic voting systems. 2016.

[20] Vera, Victor Daniel Gil; Vera, Juan Carlos Gil, Organizational Computer Security: a simulation model based on system dynamics. Scientia et technica, 2017, vol. 22 No 2, p. 193-197.

[21] Rocha Morales, Victor; Ruiz Hernandez, Oscar; Fernandez Martinez, Luis Felipe. Audit mechanism for the detection of vote tampering in electronic voting systems. PAAKAT: Technology and Society Magazine, 2018, vol. 8, No. 14.

[22] Of White, David Y. Marcos; ALONSO, Luis Panizo; ALONSO, JA Hermida. Development of an advanced methodology for evaluating Remote Electronic Voting Systems. 2016.
[23] LOPEZ, Magdalena. "Democracy in Paraguay: "The interruption of the process of change" with the dismissal of Fernando Lugo Méndez (2012). CENDES Notebooks, 2014, vol. 31, no. 85, p. 95-119.
[24] Valencia Tello, Diana Carolina; Chueiri Karam, Vera. Accountability, Reporting, And Management Control. How Does This Work in Argentina According to the legal System in Force? Legal Opinion Magazine, 2016, vol. 15, no. 29, p. 165-185.
[25] Montalvon Calderon, Aricka, et al. E-vote in the field of local administrations 2015.
[26] Legon, Carlos Miguel, et al. New probabilistic model in graphic authentication. ISSN Electronic, Automation and Communications Engineering Magazine: 1815-5928, 2019, vol. 40 no 3, p. 92-104.
[27] Of White, David Y. Marcos; Alonso, Luis Panizo; Alonso, JA Hermida. Development of an advanced methodology for evaluating Remote Electronic Voting Systems. 2016.