REVISTA ODIGOS

Período febrero - mayo 2021
Vol. 2, Núm. 1
rodigos@uisrael.edu.ec
https://doi.org/10.35290/ro.v2n1.2021.405 • e-ISSN: 2697-3405

Vulnerabilities and securities in the electronic voting: a review

Fecha de recepción: 10-01-2021 • Fecha de aceptación: 29-01-2021 • Fecha de publicación:10-02-2021

Estefanía de las Mercedes Zurita Meza[1]
Instituto Superior Tecnológico Pelileo, Ecuador.
ezurita@institutos.gob.ec
https://orcid.org/0000-0001-5509-0152

Darwin Stalin Ramírez Supe[2]
Universidad Técnica de Ambato, Ecuador.
dramirez8774@uta.edu.ec
https://orcid.org/0000-0003-0568-6489

ABSTRACT

This paper presents a study of vulnerabilities, risks, considerations and securities that can occur in a system of electronic voting in an election process of any authority. It is proposed to make an analysis as an electronic voting system can impersonate the vote traditional manual that is used for several decades in all cities of the world, these systems must ensure the integrity and proper use of the data and information obtained, but some occasions not taken into account the security considerations that are necessary in this class of systems. For this, an analysis of the security provided by electronic voting system is made as well as the vulnerabilities that may occur during the election process and some considerations to consider about electronic voting.

KEYWORDS: electronic voting, security, risk, vulnerability, encryption

RESUMEN

En el presente artículo se realiza un estudio sobre las vulnerabilidades, riesgos, consideraciones y seguridades que pueden darse en un sistema de votación electrónica para un proceso de elección de

cualquier autoridad del país. La investigación propone hacer un análisis, ya que este sistema electrónico puede suplantar al manual tradicional de votación que se utiliza desde hace varias décadas en todas las ciudades del mundo, estos sistemas deben garantizar la integridad y el uso adecuado de los datos e información obtenida, pero en algunas ocasiones no se tienen en cuenta las consideraciones de seguridad que son necesarias en esta clase de sistemas. Para ello, se hace un análisis de la estabilidad que proporciona el sistema computarizado, así como de las vulnerabilidades que pueden presentarse durante el proceso de elección y algunas consideraciones a tener en cuenta sobre la votación electrónica.

PALABRAS CLAVE: voto electrónico, seguridad, riesgo, vulnerabilidad, encriptación

Introduction

During the last decades, made the election process and to define as a means of freedom of expression to elect any authority, from the use of colored balls to ballots with candidates' graphs, manual vote achievement satisfy this human need. Over time, the technology also haves a presence in this area, at the end of the century XIX were the first mechanical voting machines in the United States (SmartReview, 2015). Since that first experience, electronic voting systems has evolved and improved functioning.

When we speak of electronic voting, we are referring to two concepts. On the one hand, the vote, as a mechanism through which citizens, living together in a representative demonstration, elect their representatives. On the other hand, the adjective electronic directly linked to the use of computer technology. It is then an information system where the value of data in particular acquires a vital importance linked to democracy and citizen rights.

Actually cover the impression of a voting receipt, verification of the votes cast, change language in the user interface (Gritzalis, 2003), and although the manual vote continues to be used, more and more countries evaluating the different technologies that exist in the market through voting drivers.

Figure 1 show how the voting process has changed from manual to electronic voting.

Figure 1. *Evolution of vote*
Source: *SmartReview (2015)*

Electronic voting is considered as a means to improve and strengthen democratic processes in modern information societies (Gritzalis, 2002)e-voting should be technically implemented in such a way that ensures adequate user requirements. As a result, the aim of this paper is twofold. Firstly, to identify the set of generic constitutional requirements, which should be met when designing an e-voting system for general elections. This set will lead to the specific (design. But, being a system in which large amounts of data and highly important information is generated there are certain vulnerabilities that should be analyzed to ensure that data are not manipulated by others outside the election process.

In the article “Risk of E-voting” of the authors Matt Bishop and David Wagner, performs an analysis of electronic voting systems in the state of California, United States of America in 2007. The results were that no system met the basic safety principles such as: confidentiality, integrity, availability. Many failures were in elementary errors such as the buffer overflow process and method of cryptography used was not suitable (Bishop & Wagner, 2007).

However, in the article “Electronic Voting” of Author Ronald L. Rivest, mentions that in electronic voting what to consider are security issues on the platform, states that any Windows or Linux does not provide the necessary security as it could be infected with virus or trojans that might alter the information (Gerck et al., 2002). For all the above mentioned it is very important to make a study of vulnerabilities and security that can offer electronic voting system.

Methodology

Being a literature review, the methodology is based on the search for papers that answer the following questions: What is electronic voting? What types of security should be considered? What are the main risks? and to guarantee the quality of the references, we chose to use scientific databases such as Google Scholar, IEEE, ScienceDirect, etc.

The following is a description of the findings:

2.1 Electronic voting

Electronic voting consists of the issuance of votes by electronic means, as opposed to traditional media are like the face vote on paper and mail voting. Technologies for electronic voting can include punch cards, voting systems using optical scanners and specialized vote places. *Figure 2* shows an electronic vote system currently used.

Figure 2. *Electronic Voting System*
Source: *SmartReview (2015)*

The purpose of this system is to make the voting process fair and transparent and it should follow some vital standard in order to achieve the integrity of the election process: first, an electro should vote only once in each election; second, electronic voting systems should support an audit log containing the vote records to detect errors and modifications. The third standard express that voters' preferences should be confidential. Fourth standard is that voting systems should be protected from fraud and exchange. The last standard is that vote results should be recorded and shown precisely exchange (Javaid, 2014). *Figure 3* shows an electronic voting system architecture.

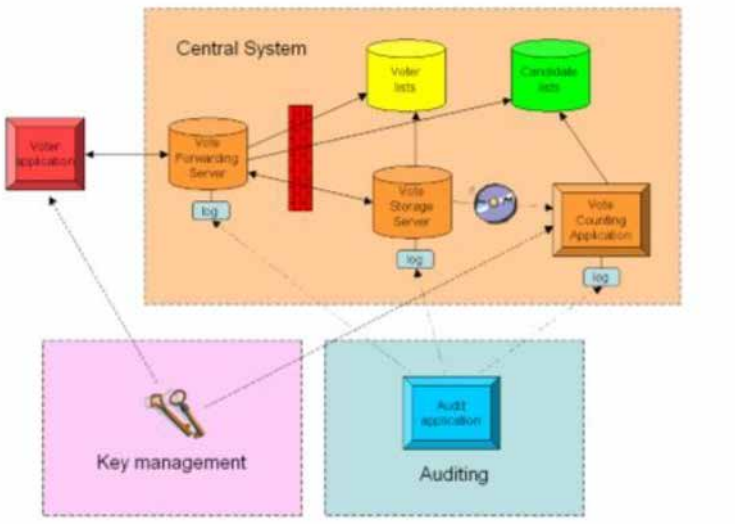

Figure 3. *Electronic Voting System Architecture*
Source: *Javaid (2014)*

It can also refer to the transmission of ballots and votes via telephone, private computer networks or the Internet. Also, can accelerate the counting of ballots and can provide improved accessibility for voters with disabilities. However, there are controversies about that electronic voting may already facilitate electoral fraud or the violation of secret suffrage (Panizo, 2007).

Many questions about the real need to use technology to solve the electoral process. Its proponents emphasize the advantages and minimize the disadvantages. Some of these aspects are indisputable, but others give safe even without basic studies on the subject. On the positive side they emphasize both accuracy and speed, and the lack of negative information security (Altman & Klass, 2005).

Among the positive arguments include issues such as accurate accounting of votes, speed count, increased accessibility for people with special needs, saving paper, flexibility, ability to create a permanent infrastructure for the opinion to vote, improving efficiency, among others. Some advantages are also considered more controversial aspects such as ecological saving, because the polls have a certain energy consumption in their manufacture and (Altman & Klass, 2005).

As for the disadvantages are also varied and some not yet demonstrated, as could be the cost of

the electronic system. The truth is that in general the security of the voting process is in question and concluded that the technology is too risky. It was a serious error of developers and researchers of systems and programs consider the level of security of electronic voting is similar to that required by a financial system, in this, the secrecy of the operation can be known by authorized third parties and instead, electronic voting, anonymity is essential part of it, so no one can have information about voting except in the final process of counting and exclusively for accounting.

2.2 Security in electronic voting systems

The electronic voting systems are being introduced, or being tested in several countries to provide more efficient voting procedures. However, the security of electronic elections has been seriously questioned (Kremer et al., 2010).

According to the Hosp and Vora theorem, there is no voting system (electronic or otherwise) that has the properties of perfect integrity, verifiability and perfect privacy at the same time. Understanding by perfect integrity the null possibility of alteration of the system, in other words, the ability to resist any malicious attempt to be modified (Nardi & Maenza, 2017).

About this approach, thinking of a system that is invulnerable seems to be a utopia, however it is possible to try to take the necessary considerations and precautions to minimize the chances of being attacked (Nardi & Maenza, 2017). *Figure 4* shows a proposed secure architecture.

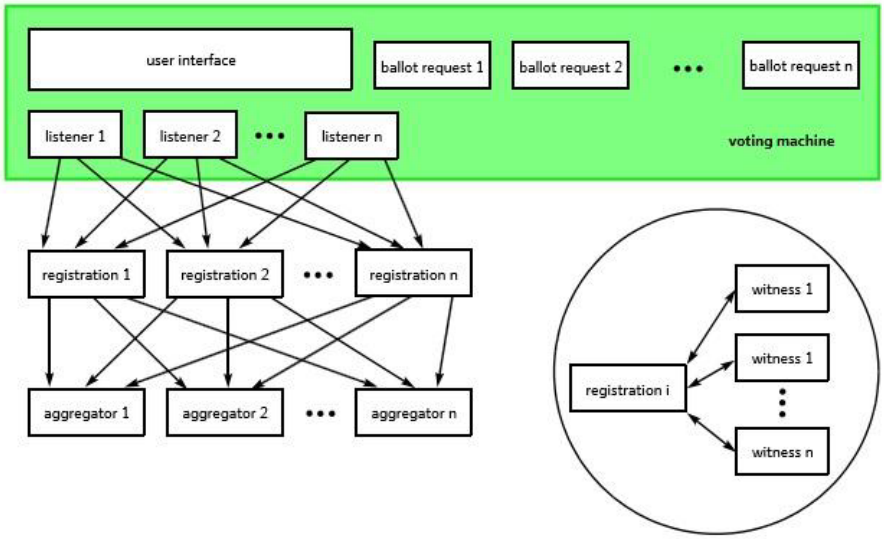

Figure 4. *Proposed secure architecture*
Source: *Nardi & Maenza (2017)*

The security that can provide an electronic voting system is the use of information systems and cryptographic schemes in order to reduce costs and human errors, and increase processing speed, without neglecting the safety of the process. However, in this type of process it is necessary to ensure the following properties (Cetinkaya & Deniz, 2007)because of the importance of the voters' privacy and the possibility of frauds. Electronic voting (e-voting:

- **Privacy**: The vote should not be associated with the person.
- **Eligibility**: Only eligible voters participate in the voting process.
- **Uniqueness**: Only one vote should be counted for each voter.
- **Uncoercibility**: No entity should be able to know the decision of the voter or to coerce it to force vote for a particular candidate.
- **Fairness**: No partial tally is revealed before the end of the voting period to ensure that all candidates are given a fair decision. Even the counter authority should not be able to have any idea about the results
- **Transparency:** The voting process should be transparent to any participating entity.
- **Accuracy**: All votes cast must be considered in the final bill.
- **Robustness:** No entity within the voting process must be able to interrupt the process from start until it reaches its end.

The proposed solutions aimed at ensuring these properties, focus on the use of cryptographic primitives based on Public Key Cryptography PKC, which offers high flexibility in key agreement protocols and authentication mechanisms. However, when the PKC is used, PKI Public Key Infrastructure is needed, to bind public keys to their owners and to allow other entities verify these unions. As a result of this, the (Kuhn et al., 2001) components of each protocol increases considerably, and a lot of computer time and storage is required when the number of features increases, *Figure 5* show the public key encryption.

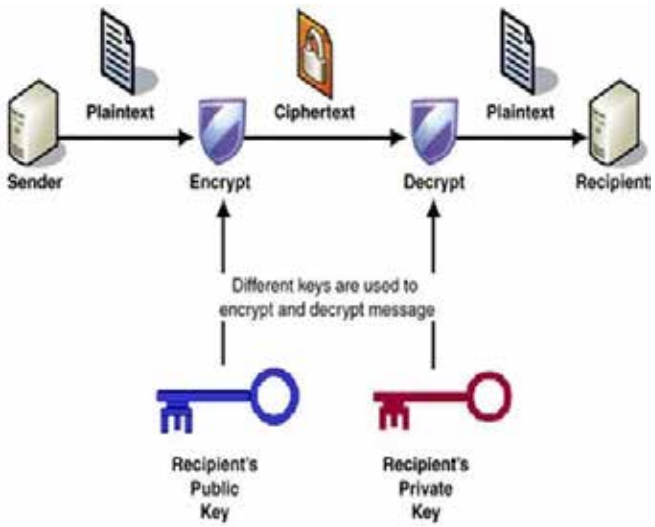

Figure 5. *Public Key Encryption*

Source: *Kuhn et al. (2001)*

Other security is to use electronic voting protocol that guarantees privacy, transparency and robustness using the properties of the bilinear pairings and use a scheme Identity Based Cryptography (Gallegos-García et al., 2010), in *Figure 6* you can see the Identity based encryption.

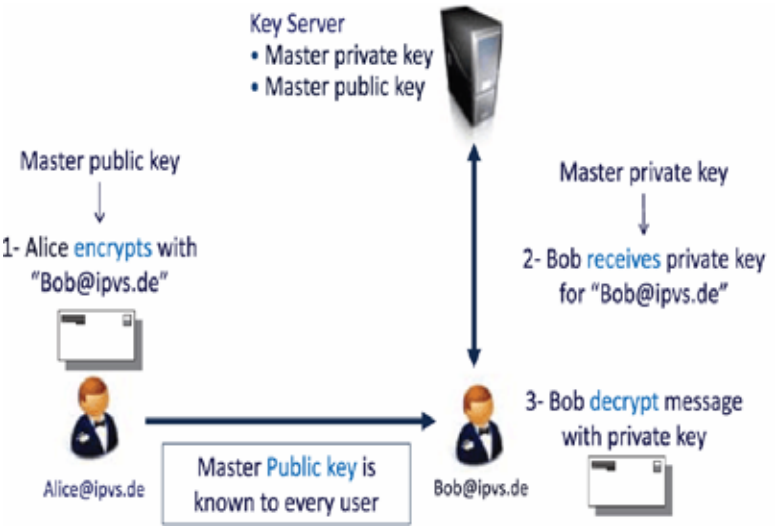

Figure 6. *Identity-based encryption.*
Source: *Gallegos-García et al. (2010)*

An electronic voting system, well designed, allows more audits than a manual system. An automated choice will always be more accurate than a manual choice.

2.3 Risks in electronic voting

By using the electronic voting new problems that do not exist in a manual voting they appear as:

- **Attacks on the database:** It allows intruders to obtain information about the votes and voters and even change the election results (Montejano et al., 2014).
- **Attacks on communication channels:** The answer to this problem is strictly cryptographic (Sterbenz et al., 2010)
- **Difficulty maintaining anonymity:** Electronic votes are stored on magnetic media and therefore is difficult to ensure that it is not any unauthorized copying. People with time and resources could work on decoding and end relating to one vote with the issuer. In manual voting that does not happen because the votes are burned past certain time (Van De Graaf et al., 2013).
- **Inconvenience to ensure transparency**: Electronic systems exist in parts of the process that cannot be con- trolled easily.
- **Naturally people tend to distrust an electronic scheme.**

The confidence of society on the system used appears to be a central point to achieve acceptance. The requirement in this regard is very significant given the importance of what is at stake in an election.

A problem that happened recently is that a user found a bug in the system that allowed to vote multiple times, this happened in Argentina with the electronic voting system called “vot.ar”. In table where the president gives each registered voter in the register a ballot, this tag contains a radio frequency identification (RFID), formed of an integrated circuit (“chip”) and an antenna. By electronic voting machines, the voter chooses the candidates of their choice, and this choice is recorded on the chip and printed on the ballot, which is then deposited in a traditional urn. The system through a study it was discovered that this process is not properly implemented, and through a programming error you can record the chip using a simple smartphone so that it contains multiple votes to the same candidate (Alonso, 2015).

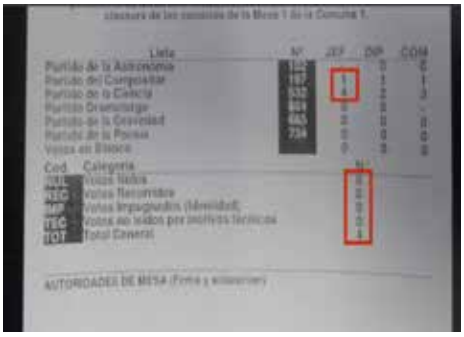

Figure 7. *Certificate with total votes*
Source: *Alonso (2015)*

In several countries also it had problems was to use electronic voting systems, which are mentioned below (Montes et al., 2016)provincial y municipal:

- **Brazil**: Using obsolete cryptographic algorithms, failure to use encryption mechanisms
- **Germany**: The systems used until now declared unconstitutional.
- **United States**: Multiple errors in various states. In several Electronic Voting was discontinued.
- **India**: Hackers are able to manipulate the results with a cell.
- **Netherlands**: Evaluate a pilot system in elections and determined that it could not guarantee the integrity of any election that will use that system. Cost of the experiment: 54 million euros.

Other European countries carried out similar experiences, subsequently going back in their implementation, to consider the cases of the Netherlands, Finland, Ireland and the United Kingdom (Nardi & Maenza, 2017). On the other hand, they were made studies where the serious security flaws presented by the system could be observed issue, generating much controversy and the refusal to continue using this system.

Is widespread belief that every social system can be migrated to a computer system, and that this automatically implies an improvement in terms of agility and economy without compromise. There are certain applications, with critical requirements of security, privacy and usability, for which current technology still cannot answer. These systems are complex and the greater the complexity, the greater the risk of failure.

Results

Electronic voting is different from e-commerce in several important ways, so it is insufficient to argue that the secure electronic voting is similar to electronic commerce and that the same security mechanisms should be applied.

For example, in e-commerce there is always time for a transaction if something did not work correctly. With the vote, there is a deadline that must be met (Gerck et al., 2002).

Based on the findings, the following important considerations in electronic voting can be mentioned:

3.1 The voting system should be simple to understand and operate. Electronic voting systems are often complex

Voting systems should be understandable and attractive to users, also they must be certified before being used. Election officials must have confidence that the voting system will prevent fraud and operate reliably.

The main purpose of a voting system is correctly determining the will of the voters. Given human nature, the probability of getting an incorrect result is much greater if there are significant security vulnerabilities if the vote count is a bit incorrect (Gerck et al., 2002).

3.2 The ability to handle disabled voters will become increasingly important.

Existing voting systems tend to be poor at accommodating the needs of disabled voters. For example, blind voters have had to trust election officials to read the ballots and enter their votes. Electronic voting systems are capable of supporting a diversity of interfaces to the voter (Panizo, 2007).

3.3 Social Engineering

Social engineering is the term used to describe attacks that involve tricking people to involuntarily commit their own safety. Talking to election officials, one discovers a problem they face is the inability of many people to follow simple instructions. For example, it is surprising to know that when you are instructed to enclose the name of a candidate, many people stress (Rubin, 2002).

Currently electronic voting could be an excellent option in COVID-19 pandemics. One of the main means of transmission of the coronavirus is the agglomeration of people, that is why changes in the voting system are analyzed to prevent the vote from becoming a focus of reactivation of infections.

> Online voting has never faced a situation as favorable as today. Amid the pandemics time, online voting is increasingly becoming the most logical solution for all types of elections. At the national and local level, the speed of innovation in special voting arrangements is unprecedented. Electoral management bodies all over the world are pondering how to adapt to the new normal, and how to address some of the risks associated with organizing elections during the pandemic (Fernandez, 2020).

The success or failure of the use of technological tools in elections, particularly electronic voting, depends, to a large extent, on the idiosyncrasy of each country, its political conditions, its development, tradition and electoral practice. These decisions cannot be taken unilaterally or behind closed doors, there must be an open consultation process that includes all relevant stakeholders.

Some countries such as Mexico, Brazil and Argentina have in recent years the use of electronic voting in electoral processes. Other countries such as Ecuador that have considered pilot projects and legislative initiatives in order to institute these tools as a fundamental component of representative democracy. For the February 2021, Ecuador has initiated three pilot plans for subsequent approval. But, there are certain doubts about the clarity and transparency of this process. However, the situation at the global level makes the processes evolve at the political level where the electronic voting system would be an appropriate option considering the current situation of the COVID-19 pandemic.

It is essential that any alternative that is considered complies with the necessary public testing and instrumentation programs and is detailed and careful to preserve confidence in the choice.

Conclusions

Electronic voting systems promise benefits in terms of ease of use and access, especially for voters with disabilities, also allowing time savings used to make the voting process. This system represents a major substantive leap in the constant task of perfecting the representative democracy, incorporating the highest technology as a tool to assure the sovereign will and transform the conventional way of conceiving and organizing an electoral process.

From the field of security of information systems, it is assessed that the risks introduced electronic voting in terms of accidental mistakes or malicious scale and easy attacks to cover up comfortably exceed the actual benefits or perceived automating a critical step of the electoral system.

The benefits associated with electric voting, in addition to saving time, in the reduction in costs that this process entails and with higher priority the health of citizens avoiding possible infections considering the current situation. This process faithfully reflects the will of the voter, without giving rise to interpretation of the vote.

References

Alonso, C. (2015). *Un informático en el lado del mal: Resultados de la búsqueda de Ataque multivoto*. https://www.elladodelmal.com/search?q=Ataque%09multivoto

Altman, M., & Klass, G. M. (2005). Current Research in Voting, Elections, and Technology. *Social Science Computer Review*, *23*(3), 269–273. https://doi.org/10.1177/0894439305275849

Bishop, M., & Wagner, D. (2007). Risks of e-voting. In *Communications of the ACM* (Vol. 50, Issue 11, p. 120). https://doi.org/10.1145/1297797.1297827

Cetinkaya, O., & Deniz, C. (2007). *Verification and Validation Issues in Electronic Voting*. The Electronic Journal of E-Government. http://www.ejeg.com/search/index.html?name=keywords&value= verification

Fernandez, A. (2020, May 3). *Transforming political parties in the middle of a pandemic: The moment for online voting? | International IDEA*. https://www.idea.int/news-media/news/transforming-political-parties-middle-pandemic-moment-online-voting

Gallegos-García, G., Gómez-Cárdenas, R., & Duchén-Sánchez, G. (2010). Protocolo de votación electrónica basado en emparejamientos bilineales. *Revista Facultad de Ingenieria Universidad de Antioquia*, *56*, 234–244. https://revistas.udea.edu.co/index.php/ingenieria/article/view/14672/12827

Gerck, E., Andrew Neff, C., Rivest, R. L., Rubin, A. D., & Yung, M. (2002). The business of electronic voting. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *2339*, 243–268. https://doi.org/10.1007/3-540-46088-8_21

Gritzalis, D. A. (2002). Principles and requirements for a secure e-voting system. In *Computers and Security* (Vol. 21, Issue 6, pp. 539–556). Elsevier Ltd. https://doi.org/10.1016/S0167-4048(02)01014-3

Gritzalis, D. A. (Ed.). (2003). *Secure Electronic Voting* (Vol. 7). Springer US. https://doi.org/10.1007/978-1-4615-0239-5

Javaid, M. A. (2014). Electronic Voting System Security. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393158

Kremer, S., Ryan, M., & Smyth, B. (2010). Election verifiability in electronic voting protocols. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6345 LNCS*, 389–404. https://doi.org/10.1007/978-3-642-15497-3_24

Kuhn, D. R., Hu, V., Polk, W. T., & Chang, S.-J. H. (2001). *Introduction to public key technology and the federal PKI infrastructure*. https://doi.org/10.6028/NIST.SP.800-32

Montejano, G., García, P., & Silvia Bast, ; (2014). *Análisis de la integridad de datos en Sistemas de e-Voting*. http://www.unsl.edu.ar

Montes, M., Penazzi, D., & Wolovick, N. (2016). Consideraciones sobre el voto electrónico. In *Repositorio Institucional de la UNLP*. http://sedici.unlp.edu.ar/handle/10915/58355

Nardi, J., & Maenza, R. (2017). *Voto Electrónico, Vulnerabilidades y Soluciones para Evitar Ataques*. https://www.researchgate.net/publication/321182889_Voto_Electronico_Vulnerabilidades_y_Soluciones_para_Evitar_Ataques

Panizo, A. (2007). *Aspectos tecnológicos del voto electrónico* (Documento de Trabajo N.° 17). https://www.researchgate.net/publication/259668840_Aspectos_tecnologicos_del_voto_electronico

Rubin, A. D. (2002). Security considerations for remote electronic voting. *Communications of the ACM*, *45*(12), 39–44. https://doi.org/10.1145/585597.585599

SmartReview. (2015). *Voto Manual vs Voto Electrónico*. https://es.slideshare.net/smartmatic/voto-manual-vs-voto-electrnico

Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, *54*(8), 1245–1265. https://doi.org/10.1016/j.comnet.2010.03.005

Van De Graaf, J., Montejano, G., & García, P. (2013). *Optimización de un esquema "Ocuppancy Problem" orientado a E-Voting*. http://www.dcc.ufmg.br/~jvdghttp://www.unsl.edu.ar