




Electronic Voting System for Universities in Colombia

Jose Llanos¹^a, William Coral²^b, Alvaro Alarcon¹^c, Juan Cruz²^d and Jhojan Ramirez²^e

¹Department of Computer Science, Corporación Universitaria del Huila - CORHUILA, Neiva, Colombia

²Department of Mechatronics Engineering, Corporación Universitaria del Huila - CORHUILA, Neiva, Colombia

Keywords: Election Process, Electronic Voting Systems, MVC, OWASP.

Abstract: In this manuscript we present the development of Electronic Voting System (EVS) for the elections process at universities in Colombia. This application is based on the architectural pattern Model View Controller (MVC) and Open Web Application Security Project (OWASP) by defining five risk associated to the security of the system. During the development of this software we performed a wide range of usability tests and response times. This allowed to improve the performance of this software in its execution and delivery of results. We conclude that the use of this type of applications allows to obtain the results quickly and accurately and the process of recount votes is eliminated and the costs of executing the electoral process are reduced.

1 INTRODUCTION


The voting method is a vital part of the democratic process in any organization (Olaniyi et al., 2013). It contains a series of elements that allow democracy to be exercised through the election of political parties that represent the population (Ayala et al.,). The traditional election process is expensive, slow and need complex preparation (Hussien and Aboelnaga, 2013). Electronic voting refers to the use of computers or computerized voting equipment to cast their vote in an election (Mohammed and Timour, 2013). As well an electronic voting system is a system that registers electoral data and processes them mainly as digital information (Al-Ameen and Talab, 2013). Its goal is to improve the accessibility, precision and security of the elections in order to optimize the democratic process.


Electronic voting has many advantages over the traditional way of voting. Some of these advantages are the lower cost, faster tabulation of the results, better accessibility, greater precision and a lower risk of human errors. As well the electronic voting system needs to fulfill with some requirements for its implementation (Hussien and Aboelnaga, 2013) - (Al-Ameen and Talab, 2013), these are:


- **Eligibility:** Only authorized voters who meet a predetermined criteria can vote (Hussien and Aboelnaga, 2013).
- **Singularity:** No one can vote more than once (Hussien and Aboelnaga, 2013).
- **Privacy:** A vote is kept secret and no one can determine your choice (Hussien and Aboelnaga, 2013).
- **Integrity:** The electoral process is safe, so nobody can change the vote of another person without being discovered (Hussien and Aboelnaga, 2013).
- **Accuracy:** Each voter can ensure that their vote has been taken into account in the final tabulation (Hussien and Aboelnaga, 2013).


In this project the EVS was include to improve the security of the system by restricting access for people who are not authorized in the database. In this way we can offers greater reliability of the results obtained by the election committee. Likewise it allows to carry out the suffrage action in a friendly and interactive way.


Around the world, the EVS has been implemented successfully and several countries have changed their paradigms of the old classical method for systematized electoral processes. Brazil has been implementing the electronic voting with a good results and at the same time have been vital for the improvement of its electoral and political system (Pérez Duharte, 2013). Among the main advantages that are perceived with electronic voting are security, speed, reliability

^a  <https://orcid.org/0000-0003-4642-2770>

^b  <https://orcid.org/0000-0002-3971-9536>

^c  <https://orcid.org/0000-0003-4703-1907>

^d  <https://orcid.org/0000-0002-3851-8732>

^e  <https://orcid.org/0000-0002-6863-5200>

and the possibility of correction (Bonifaz, 2014). In the last years in Colombia some applications for the electoral process have been implemented at the level of universities and colleges. This thanks to the law (law 892 of 2004) (Giraldo, 2007) that regulates the electronic mechanism of registration and electronic voting through the support and implementation of a computer system (Mendoza Suarez et al., 2016). However, this process has been implemented only in a very few cities. In the south of Colombia where our university is located this kind of software has not been implemented before this work.

The rest of the paper is organized as follows. Section 2 provides a detailed description of the software development. Section 3 describes the evaluation of usability and the response times of the application. The Section 4 delivery the results. The conclusions are sketched in Section 5 and future work in Section 6.

2 SOFTWARE ARCHITECTURE

EVS incorporates people, electronic devices and data processing. Offers the services of visualization of results for all stakeholders. This project focuses on the development of a Web application that allows improving response times and reducing the costs of conducting the electoral process (Hussien and Aboelnaga, 2013).

To better understand the proposed solution it is necessary to analyze the architecture implemented in the software. These includes the architectural pattern Model Vista Controller (Figure 1) (Pantoja, 2004). In the Vista we find the XHTML files that are responsible for taking the user's request and sending it to the controller. This was implemented using the Managed Beans a JavaServer Faces (JSF) framework. The JSF contains the logic of the business and takes the information from the form and transfer it to the model. These is a serializable class that allows the invocation of the objects the persistence of the data and the communication with the database. When the database engine processes the request a message is returned to the model and this is delivered to the controller to finally notified through the user's view (Pech-May et al., 2011).

2.1 Security

We based the security of this project on the report made by the Open Web Application Security Project (OWASP) where the Top 10 of the Most Critical Web

Application Security Risks are listed. We implemented on the project 5 of the 10 risks detailed as follow:

- **Risk A1 - Injection:** This type of risk occurs when an attacker sends harmful information to an interpreter. The variables or parameters sent do not have the respective validation and the injection may cause disclosure, loss or corruption of the information. XML parsers and parameters can be generated in SQL queries (Singh, 2016).

The attack is prevented when the command data and queries are separated. If stored procedures are used it is necessary to use validated parameters. Concatenation and special characters must be avoided (Wichers, 2013).

In the EVS the data supplied by the user on the frontend are validated and the parameters used in the Managed Beans were adjusted for the stored procedures in order to avoid an attack through SQL queries to the base engine data.

- **Risk A2 - Lost Authentication:** In this risk an attacker can obtain the credentials by using brute force tools as well as dictionaries to break the passwords. This problem occurs when access controls and session management are not implemented. With this type of attack you can steal the identity of the users. Information that is sensitive to an organization can also be disclosed (OWASP, 2017).

This risk is prevented with multi-factor authentication and the implementation of security policies. That includes the change of credentials by default, the control of weak passwords and their rotation (Kim and Hong, 2011).

In the application Web to avoid attacks using brute-force tools or dictionaries that break the access credentials, the AES 128 algorithm was implemented to encrypt (peer-to-peer) the connection parameters with the database. The SHA-512 algorithm for encrypting user passwords and security policies for password change were defined (McLoone and McCanny, 2002).

- **Risk A5 - Loss of Access Control:** The exploitation of access control is very often used by attackers. This type of attack is very common because it requires automatic detection and the use of effective functional tests by application developers. The impact of the attack let the system to act as administrator using privileged functions that allows you to create, access, modify or delete any record (OWASP, 2017).

To prevent this attack it is necessary to configure the server in order to verify access control

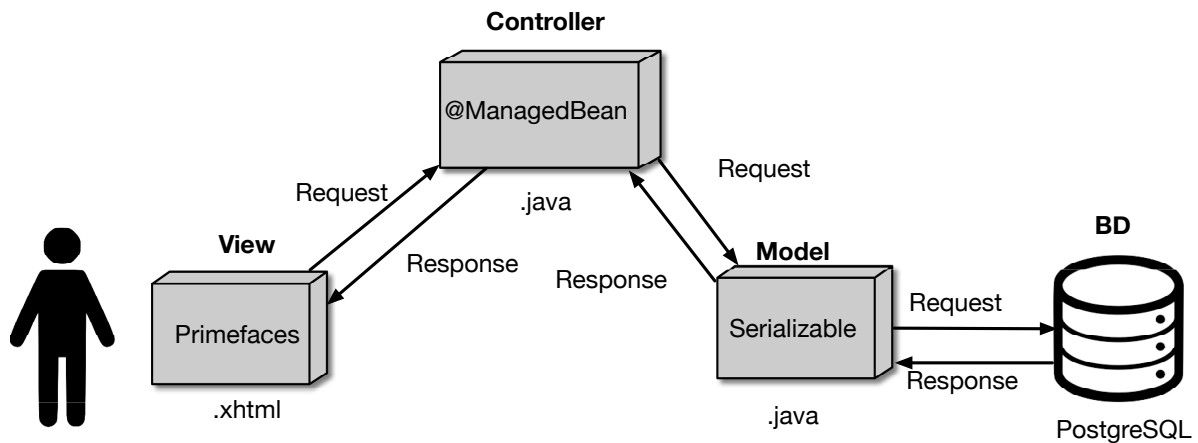


Figure 1: The figure shows the MVC architectural pattern implemented in the EVS. The Vista are .xhtml files that contain rich Primefaces components. Here the user interacts with the Web application through a browser and generates their requests to be sent to the controller. The Controller is a ManagedBean class that receives the requests generated by the View and passes them to the Model. The Model is composed of a serializable Java class. This class is in charge of receiving the Controller's request to pass it to the database engine that processes it. Finally, it returns the generated response to the Controller so that it can be shown to the user through the View.

or metadata. HTTP access control must be minimized. Web server directories must be disabled and developers must apply access control and integration tests (OWASP, 2017).

In the application Web to avoid anonymous attacks that allows the disclosure, modification or destruction of the data, we use secure URLs, MAC and IP validation in all the equipment involved in the process. Likewise, we include in the whole process a transaction log that allows verified and to control the transactions used during the deploy of the application.

- **Risk A6 - Incorrect Configuration and Security:** In many cases attackers try to access applications through unused pages, unprotected files and directories. This type of attack occurs because there are incorrect configurations in the security of the network, the application server and the databases. The main objective of this type of attack is to obtain unauthorized access to the data and functions of the Web application. They also generate this process in order to obtain system and business information (OWASP, 2017).

In order to prevent this attack it is necessary to implement development and production environments with the required security elements. It is important not to install features that are not required. The configurations must be updated based on a patch management process. The application must handle a segmented architecture that guarantees an effective and safe separation of the components (Medvidovic and Taylor, 2000).

In order to avoid vulnerabilities of unused pages,

unprotected files and directories, a segmented network with no Internet access defined only by the teams involved in the election process was defined. Security policies were also defined for the server, the PostgreSQL database engine and the application server.

- **Risk A10 - Insufficient Registry and Monitoring:** This attack is the basis of all large security incidents. Due to the constant monitoring is not carried out on the different systems the attackers takes advantage of this situation to achieve their objectives without being detected. Successful attacks begin with exploiting vulnerabilities and identifying gaps (OWASP, 2017).

To prevent this type of attack it is important to verify all the existing login and access controls. Constantly verify high-impact transactions and include audit and integrity controls that allows the timely identification of any eventuality in database records. Finally define a security policy to respond to the timely recovery of incidents (Kohno et al., 2004).

In our project to avoid security incidents and the exploitation of vulnerabilities in the Web application we used audit tables made in the database. In this way these tables monitor records, successful and failed logins and transaction control made or declined during the voting process.

We consider that the risks listed before are the most relevant for these web application. However, we know that our software are vulnerable as well to the other risks.

3 VOTING DESCRIPTION

The EVS developed on this project and describe in this section has two parts. The first is about the components involved on the web application and the second handle with the voting process follow by the user to register its votes.

3.1 Components

The Web application consists of 11 modules that have been designed and implemented in order to allow the development of a complete electoral process.

- **Module 1 - Electoral Committee:** This module will create and modify the electoral committee, committee positions and role descriptions, delegates and the electoral committee minutes.
- **Module 2 - Registration:** This module creates and modified the agreements, the resolutions for the election, the type of election to be made, the applicant's requirements and the documents that must be submitted, the election and its respective schedule.
- **Module 3 - Formulas:** This creates the voting formulas and proposals of the voters.
- **Module 4 - Voters:** In this module voters are created and associated to the respective formulas registered for the electoral process.
- **Module 5 - Juries:** The respective juries are created and assigned the headquarters, the schedule and the table in which they will participate.
- **Module 6 - Manuals:** In this module you will find the user, installation and deployment manuals of the Web application.
- **Module 7 - Elections:** The voter is activated to allows carrying out the electronic voting.
- **Module 8 - Proceedings:** The elector is activated to perform the voting process.
- **Module 9 - Reports:** This generates the reports of aspirants, voters, results and the verification report of the electoral process.
- **Module 10 - Configuration:** We set-up the campus for the election, the faculties, the tables, the programs, the campus, the type of document, the type of formula, the university, the type of link of the teachers, the computers and the rooms that will be used for voting.
- **Module 11 - Security:** Users and profiles are configured in this module.

3.2 Process

In this section we are going to describe the process follow by the users to vote using our EVS. This process was developed based on the law 892 from the electoral committee of Colombia (Giraldo, 2007). Likewise, the steps follows by the voters take into account the needs from each University.

The voting process begins when the electoral committee generates an agreement that describes the importance of the voting process for the institution. Then a resolution is generated that describes the type of election to be developed. This resolution includes the requirements and documents that applicants must present, the schedule of activities and the election day. Subsequently, the applicant performs the registration process, the delivery of documents and the definition of the Electoral Formula that consists of a principal candidate and a substitute candidate. When the registration process of the formulas is completed the closing act of the registration is generated. The forms used for the configuration of the electoral process defined previously are describe as follows:

- **University Campus:** In this form we create the campus that currently has the university around the country.
- **Faculties:** Here we can configure the faculties that currently has the university.
- **Voting Tables:** In this form we configure the tables used in the electoral process. Every tables is associated to one faculty and one campus.
- **Program:** It allows to configure all the academic programs that the university has available for its academic offer.
- **Types of Documents:** Here are loaded the documents required by each candidate.
- **Types of Formula:** This allows the user to configure the formulas with their respective candidates.
- **Computers:** Describes each of the computers that will be used in the electoral process with their respective IP and MAC addresses.
- **Rooms:** In this form we created the rooms that are going to be used for the development of the electoral process.
- **Vote View:** In this form the elector enter with his credentials and generates the electronic vote.

Each voter was presented to the voting jury with the identity card for its activation in the Web application through a bar code reader. Then he goes to the computer designated by the jury (inside the voting room) to generate the electronic vote through the

Risk	Attack vector	Weakness of security	Prevention
A1 - Injection	Attack to parameters XML and queries SQL	Disclosure or loss of information	Parameters validation in the files XML and use of stored procedures validated
A2 - Lost Authentication	Access control and session management not implemented	Loss of credentials of access and passwords	Implement of multi-factor authentication and security policies.
A5- Loss of Access Control	Exploitation of access control	The attacker have privileged functions that allows disclosure, modification or destruction of the data	Configure the access control and the metadata in the server. The developers must apply access control and integration tests
A6- Incorrect configuration and security	Obtain unauthorized access to the data and functions of the Web application	Incorrect configurations in the security of the network, the application server and the databases	Implement development and production environments with the required security elements
A10 - Insufficient Registry and Monitoring	Exploitation of the vulnerabilities and the identified of gaps	Constant Monitoring of the different systems without being detected	implement the access control. Constantly verify high-impact transactions. Include audit and define different security policy

Figure 2: The figure shows the risks that were analyzed and implemented in the EVS based on document OWASP 2017. This document socializes the 10 most relevant attacks that Web applications have in the production environment. From these risks, the A1 corresponding to injection was selected. A2 to Lost Authentication. A5 Loss of Access Control. A6 Incorrect configuration and security. A10 Insufficient Registry and Monitoring.

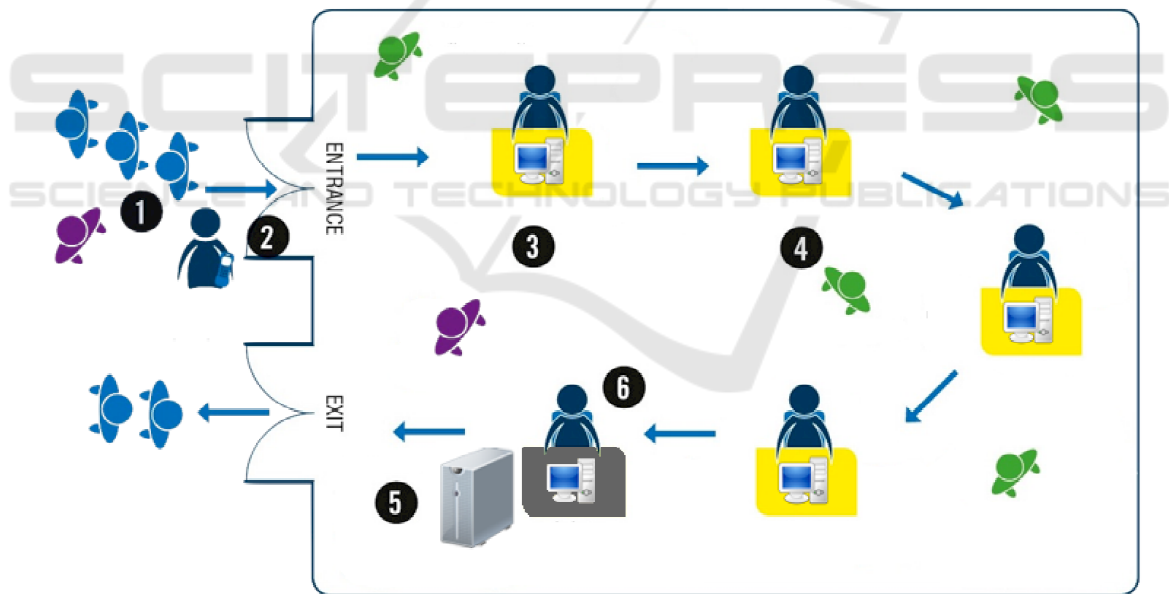


Figure 3: 1. The voter arrives in the voting room. 2. The jury activates the voter through identity card, so that they can generate the vote in the EVS. 3. The voter generates the vote in the EVS. 4. Viewers keep the voting room in order. 5. The vote is stored on the server. 6. The jurors verify the status of the vote and generate the labor certificate.

Web application. Finally the jury verified in the application if the vote had been registered through a vote counter and gives the voting certificate to each voter.

The electronic voting process was carried out during a single day. At the end of the day the process is close and the following reports are generated:

- **Results:** This report shows the results of the electronic voting organized by voting table and venue for each formula registered in the electoral process.
- **Act of Voters:** This record shows all the people who made the electronic vote in their respective

polling station and headquarters.

- **Act of the Electoral Committee:** It allows to visualize all the people that are part of the electoral committee with their respective functions and responsibilities.
- **Act of Verification of Results:** This act allows auditing the results obtained in the electronic voting process.

Finally the Web application gives the results and the candidates who gets more than half wins. Likewise the application gives the names and the ranks of the others candidates.

4 EXPERIMENTAL TEST-BED SETUP

For the development of the electronic voting process, a room with one server and five desktop computers is configured. The Web application and the database were implemented on the server. A desktop computer is responsible for carrying out the voting process.

The test-bed is composed by two parts hardware and software. This allows the implementation, deployment, electronic voting and delivery of results.

4.1 Hardware Components

Within the hardware components we found a server where the Web application is deployed. Likewise, the desktop computers where the electronic voting process is performed and where the jury activates the voter to carry out the voting process are considered as part of the hardware.

All the computers were in a LAN network with static addressing and local connection to the server. In order to avoid attacks or frauds to the electoral process.

1. Server.

For the deployment of the Web application, the DELL PowerEdge 830 tower server with CentOS Operating System 7 was used. This server is ideal for its flexible performance for different applications and database engines. It comes equipped with a tool for its management guaranteeing a reduced maintenance and a simpler administration. Table 1 shows the technical specifications of the server.

2. Desktop Computer.

In order to carry out the voting process and the activation of the voters, 10 desktop computers with the following specifications were used.

Form factor	Tower
Processor(s)	Single Intel® Pentium® D (dual core) processor (up to 3.2GHz) Single Intel Pentium 4 processor (up to 3.6GHz) Single Intel Celeron® D processor (2.53GHz)
Front side bus	800MHz for Pentium 4; 800MHz for Pentium D; 533MHz for Celeron
Cache	1MB or 2MB for Pentium 4, two 1MB for Pentium D; 256K for Celeron
Chipset	Intel E7230
Memory	Up to 8GB DDR2-533/667
Drive controller	Embedded SATA; optional U160
Maximum internal storage	Up to 1TB SATA or up to 1.2TB SCSI
Hard drives*	80GB, 160GB and 250GB* (7,200 rpm) SATA
Internal storage performance	10K/15K RPM U320 SCSI drives; 7200 RPM SATA drives
External storage	Dell PowerVault™ tape or SCSI
Network interface card	Single embedded Gigabit* ethernet
Power supply	420W
Availability	DDR2-533/667 ECC memory; hot-plug SCSI
Video	XGI XG20 on motherboard with 16MB memory
Remote management	Baseboard management controller; optional DRAC/4p

Figure 4: Technical specifications of the server used for the implementation and deployment of the EVS.

- **Processor:** Intel Core i5-6500
- **RAM Memory:** 8GB
- **Hard Disk:** 500GB
- **Operating System:** Windows 10 64-bit

3. Code Bar Reader.

A barcode reader was used to activate and validate the voter. This reader was implemented in each of the rooms where the voting process took place. The technical specifications of the device are as follows

- **Make:** Honeywell
- **Model:** Mk9520 Laser
- **Dimensions (LxWxH):** 198 mm x 78 mm x 56 mm
- **Weight:** 149 g (5.3 oz)
- **Input Voltage:** 5 VDC + 0.25 V
- **Operating Power:** 825 mW (165 mA at 5 V)
- **Standby Power Supply:** 600 mW (120 mA at 5 V)

4.2 Software Components

The software is composed by three elements, the application server that allows you to deploy the solution, the Web application and the database:

1. Application Server.

The application server used was GlassFish 4.1.1. This software allows to deploy WAR files (Web Application Archive) that contains the Web application, resources and reports. Then using a browser the solution is accessed through the https protocol and port 8080 (Heffelfinger, 2014).

2. Web Application.

The Web application consists of the Front End and the Back End.

Front End: The PrimeFaces 6.0 component library was used. This allows graphical interfaces to be developed from XHTML pages and providing the development of Java Server Faces (JSF) applications.

Back End: The JSF 2.2 framework was used to develop Web applications for the Java EE platform. This implements the MVC architectural pattern, managed beans and classes of serializable type (Ccalicskan and Varaksin, 2015).

3. **Database.**

The database management system used was PostgreSQL 9.4, a relational and object-oriented engine that is under the BSD license and allows the construction of robust databases with excellent performance (Juba et al., 2015).

5 **RESULTS**

The elections were represented by two formulas and the blank vote. Each form was made up of a principal and a substitute. The election process took place in two ways. Through traditional voting (manually) and through the Web application. The EVS was used in two of the three university campus proposed for the voting process. Four polling stations were implemented in each of these locations. At the first campus 25 votes were logged. In the main campus 58 votes were logged. The total number of votes generated in the application was 83.

The EVS automatically closed the voting process at 20h and all the computers that had been selected were disabled. Once the elections were over, the results report was generated and it was observed that the application took approximately 30 seconds.

The average time took for each voter with the traditional method (manual) was 73 seconds, while the average time with the EVS was 27.9 seconds. This indicates a time reduction of 45.1 seconds for each voter in the whole process. In figure 5 we can see a sample for the time expend by the voter between the two methods.

Likewise, at the end of the process the traditional voting counting starts and it took more than 1 hours for give the winner formula, created the reports and the acts for the electoral committee. Meanwhile the Electronic Voting System did everything only in 30 seconds.

In the same way, the expenses with the traditional method was reduced from \$5.000USD to \$100USD for the use of the electricity, internet, and paper sheets.

Test Number	Traditional Method Time (Second)	Electronic Voting System Time (Second)
1	75	25
2	77	30
3	73	28
4	78	26
5	71	30
6	73	29
7	74	27
8	69	28
9	71	29
10	69	27
Average	73	27.9

Figure 5: This table contains a sample of 10 voters comparing the two methods. The total of the voter who participated as volunteers was 83. Compared with the entire voters that was 159 we obtained a sample of 52.20%.

Traditional Method Time	Actions Carried Out	Electronic Voting System Time	Actions Carried Out	Percentage Improvement of time
3600 seconds	* Vote counting. * Recount of votes. * Generation of reports. * Acts for the Electoral Committee.	30 seconds	* Vote counting. * Generation of reports. * Acts for the Electoral Committee.	12000%

Figure 6: The figure shows the comparison of the time used for voting through the traditional method (manual) and the EVS. It also describes the actions carried out in each of the processes.

Traditional method expenses	Used Materials	Electronic Voting System expenses	Used Materials	Improvement percentage
\$5000USD	Stationery (ballot cards, voter list, results minutes and delivery records), advertising of the event, food for juries, transportation, hours of work of teachers	\$100USD	Electricity, paperwork (results minutes and delivery records) and hours of work of teachers	5000%

Figure 7: The figure shows the comparison of the expenses used for voting through the traditional method (manual) and the EVS. It also describes the materials used in each of the processes.

The EVS has the option of activating the voters through a barcode reader. It was used during the election process, in order to observe its functionality and verify the software response times. It is concluded that this option worked efficiently because through the institutional card the identification of each voter was read and activated automatically in the software. In this way, the waiting lines for the beginning of the electronic voting were avoided.

6 CONCLUSIONS

In this work we propose an Electronic Voting System (EVS) based on the law 892 of 2004 for the electoral process at universities in Colombia. The solution implements the registration process of the voters with their respective formulas, voters and juries. It also implements the electronic voting process and the generation of the reports with the respective results.

With the different algorithms implemented in the EVS the attack risks of the electoral process and the data stored in the database engine can be reduced. This because in the user interface the input parameters are validated and stored procedures are implemented. We also use secure URLs and MAC validation for all the teams involved in the process in order to verify and control the transactions made.

For the tests that were carried out of the EVS a segmented network without access to the Internet was defined for the teams involved in the electoral process. The purpose of this configuration is to define security policies to avoid the modification of files, directories and the database that are found in the production server.

With the tests carried out at the EVS it was identified that the costs and response times of the electoral process are significantly reduced compared to the traditional method. This because the actions carried out and the materials used in each phase of the process are optimized.

REFERENCES

- Al-Ameen, A. and Talab, S. A. (2013). The technical feasibility and security of e-voting. *Int. Arab J. Inf. Technol.*, 10(4):397–404.
- Ayala, A., Daniel, S., and Vinzoneo, M. Los procesos electorales y las nuevas tecnologías.
- Bonifaz, M. S. (2014). Percepciones de los peruanos sobre el voto electrónico presencial. *Consejo editorial*, page 99.
- Ccalicskan, M. and Varaksin, O. (2015). *PrimeFaces cookbook*. Packt Publishing Ltd.
- Giraldo, F. (2007). Partidos y sistema de partidos en Colombia. *La política por dentro: Cambios y continuidades en las organizaciones políticas de los países andinos*, pages 123–159.
- Heffelfinger, D. R. (2014). *Java EE 7 with GlassFish 4 Application Server*. Packt Publishing Ltd.
- Hussien, H. and Aboelnaga, H. (2013). Design of a secured e-voting system. In *2013 International Conference on Computer Applications Technology (ICCAT)*, pages 1–5. IEEE.
- Juba, S., Vannahme, A., and Volkov, A. (2015). *Learning PostgreSQL*. Packt Publishing Ltd.
- Kim, J.-J. and Hong, S.-P. (2011). A method of risk assessment for multi-factor authentication. *Journal of Information Processing Systems*, 7(1):187–198.
- Kohno, T., Stubblefield, A., Rubin, A. D., and Wallach, D. S. (2004). Analysis of an electronic voting system. In *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004*, pages 27–40. IEEE.
- McLoone, M. and McCanny, J. V. (2002). Efficient single-chip implementation of sha-384 and sha-512. In *2002 IEEE International Conference on Field-Programmable Technology, 2002.(FPT). Proceedings.*, pages 311–314. IEEE.
- Medvidovic, N. and Taylor, R. N. (2000). A classification and comparison framework for software architecture description languages. *IEEE Transactions on software engineering*, 26(1):70–93.
- Mendoza Suarez, C. R. et al. (2016). El voto electrónico en Colombia: análisis de viabilidad de su implementación.
- Mohammed, D. A. A. and Timour, R. A. (2013). Efficient e-voting android based system. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(11).
- Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O., and Olu-dotun, A. (2013). Design of secure electronic voting system using multifactor authentication and cryptographic hash functions.
- OWASP, O. T. (2017). Top 10-2017.
- Pantoja, E. B. (2004). El patrón de diseño modelo-vista-controlador (mvc) y su implementación en java swing. *Acta Nova*, 2(4):493.
- Pech-May, F., Gomez-Rodriguez, M. A., Luis, A., and Lara-Jeronimo, S. U. (2011). Desarrollo de aplicaciones web con jpa, ejb, jsf y primefaces.
- Pérez Duharte, J. A. (2013). *El impacto de la administración electoral en la democracia latinoamericana*. PhD thesis, Universidad Complutense de Madrid.
- Singh, J. P. (2016). Analysis of sql injection detection techniques. *arXiv.org*.
- Wichers, D. (2013). Owasp top-10 2013. *OWASP Foundation, February*.