Analysis of Appropriate Security Processes to Mitigate Risk in a Popular Election System

Segundo Moisés Toapanta Toapanta*
Department Computer Science
Universidad Politécnica Salesiana(UPS)
Guayaquil, Ecuador
stoapanta@ups.edu.ec

Christopher Eduardo Solís Salazar
Department Computer Science
Universidad Politécnica Salesiana (UPS)
Guayaquil, Ecuador
csoliss@est.ups.edu.ec

Daniel Humberto Plua Moran
Department Computer Science
Universidad Politécnica Salesiana (UPS)
Guayaquil, Ecuador
dplua@ups.edu.ec

Luis Enrique Mafla Gallegos
Faculty of Systems Engineering
Escuela Politécnica Nacional (EPN)
Quito, Ecuador
enrique.mafla@epn.edu.ec

Ma. del Roció Maciel Arellano
Department of Information System
Universidad de Guadalajara
(CUCEA) Guadalajara, México
ma.maciel@academicos.udg.mx

***Abstract*— The Consejo Nacional Electoral of Ecuador has been seriously questioned with the implementation of the System of Transmission and Publication of Results (STPR). Descriptive tables of threats and controls were analyzed; to determine criteria such as: loss of integrity, loss of availability and loss of confidentiality. The objective was to identify the security protocols, determining the processes that make up the electoral vote. The qualitative documentary analysis and impact of the analyzed threats was used. In this way the results said that the system is highly vulnerable to threats of human origin, the highest risks are the threats of computer criminals or malicious collaborators. It was concluded that the greatest risk lies in the employees, their selection and hiring must be carried out without incidents of the policy, that comply with a professional profile according to the functions or tasks that they will fulfill and that demonstrate values such as honesty and ethics.**

Keywords*— *Electoral processes, Information Integrity, Information Security, Process Security.

I. INTRODUCTION

Popular elections, for dignities or consultations with people, constitute the most important democratic exercise in society governed by this political system, but this electoral system presents multiple controversies, because there are factors that can put at risk an election. They often come from human, accidental or intentional actions [1].

The veracity of the results of the demonstration of the will of citizens at the polls is protected by efficient security protocols throughout the process. However, in Ecuador the news published by various media since the promulgation of the new Code of Democracy (2009), warn that the electoral processes have been seriously questioned by political organizations and process providers, most of them by the implementation of the System of Transmission and Publication of Results (STPR) due to the failures that this has presented especially in the access to information on the website [2].

The initial protocol that was carried out in the Consejo Nacional Electoral (CNE), begins with the stamping and zeroing of the STPR database, the sealing protocol consists of encrypting the STPR information through a code that It allows to protect, maintain and certify the integrity of the computer system. By means of this action, the filtering or the entry of information extraneous to the verification of votes will be avoided [3].

What are the suitable protocols to reduce the risks in a popularly chosen system?

To answer the research question that is the main objective of the analysis in this article, we first identify the electoral administration systems used in Latin America and specifically in Ecuador. The Karisma Foundation and its Digital Security Laboratory (KLAB) [4], describe the different types and their characteristics in an audit proposal of 2018 for the institution of the Registro Nacional de Estado Civil (RNEC) in charge of the electoral processes in Colombia.

The qualitative documentary method is used, since all the information of the specialized publications is reviewed in the risk assessment models of the electoral systems and processes. Descriptive because it relates the information based on tables.

The results of the analysis of the risks in the electoral system, is a protocol, for the selection of the personnel that works in the processes of elections of the CNE, under contract or relationship of dependence and a risk assessment of the human threats.

In the Guide of risk management for information technology systems of the National Institute of Standards and Technology, it describes what threats are their origin, motives and actions that can cause damages of various types to the system [5].

It was concluded that the greatest risk lies in the employees of the popular electoral system, their selection and hiring must be done without incidence of the policy, that they meet a professional profile according to the functions or tasks they will fulfill and that demonstrate values. Like honesty and ethics.

II. MATERIALS AND METHODS

A. Methods

The qualitative documentary analysis is the basis of this article, since all the information of the specialized publications is reviewed in the evaluation of risks of the electoral systems

Universidad Politécnica Salesiana sede Guayaquil

978-1-7281-1374-6/19/$31.00 ©2019 IEEE

and processes. It is also descriptive because it relates the information to the object of the research, which consists in analyzing the security protocols of a system of popular and explanatory choice because it characterizes the elements and models that were analyzed.

B. Materials

The evaluation of general risks was made based on the Risk Management Guide for Information Technology Systems proposed by the National Institute of Standards and Technology NIST SP 800-30 [6] through descriptive tables to find an evaluation in qualitative terms of the risks in which the popular electoral systems are immersed. On the basis of ISO standard IEC 15504 (Determination of the software process improvement capacity (SPICE) [13].

The international standard ISO / IEC 15504 is the Determination of the Capacity of Improvement of the Software Process, has as a requirement an evaluation of the capacity and / or maturity of the processes [11].

To measure the capacity of a process, a set of process attributes (Process Attributes) (PA) is used, where each attribute defines a particular aspect of the process capability. In this sense, process attributes are common to all processes and describe the characteristics that must be present to institutionalize a process.

The fulfillment of the process attributes will determine the level of capacity of the process and hence the level of maturity will be determined by the levels of capacity of all the processes associated with the level of maturity.

C. The electoral systems

Electoral management systems can be classified into manuals, hybrids and electronic. Among the hybrid systems are: the electronic voter registration, the transmission of results by magnetic or digital means and the use of applications to consolidate and publish the results. In turn, the electronic components are divided into: electronic counting through recognition software such as OCR (Optical Character Recognition) or OMR (Optical Mark Recognition), electronic voting on Direct Recording Machines (DRE) and Internet voting [2].

The Consejo Nacional Electoral (CNE) is the institution that decides on the use of electronic voting methods and / or total or partial scrutiny in the different elections in accordance with art.113 of the current democracy code [9].

The Organization of American States (OAS) granted the CNE a certification that is within the technical specification ISO / TS 17582, which is based on eight processes:

- Voter registration
- Registration of political organizations and candidates
- Electoral logistics
- Suffrage
- Checking results
- Electoral education
- Control of political financing
- Solve the electoral challenges

The process of suffrage is physical and manual through individual and secret ballots. The voting process is carried out by the miembros de la Junta de Receptores de Votación (MJRV) and the minutes with the results are delivered to the coordinators of the electoral district, who in turn deliver a copy to the data processing center and they send another one to the provincial delegations. The security in these processes is in charge of the Fuerzas Armadas (FFAA), the Policía Nacional (PPNN) and the Consejo Nacional Electoral (CNE), the requirements of the computer security protocols are applied in the STPR [10].

D. Risk analysis

According to the National Institute of Standards and Technology, to carry out risk analysis, it is necessary to review the threats that may cause incidents and material or immaterial damages in the organization, which may be:

- Human threats
- Natural threats
- Environmental threats [3]

Each of these threats comes from a source and is the product of a motivation or cause to execute an action, then the descriptive tables of human threats:

TABLE I. HUMAN THREATS

Source	Motivation	Action
Hacker, Cracker	-Challenge -Ego -Rebellion	-Hacking -Access denied
Computational Criminal	-Obtain economic return -Information divulgation -Alteration of Information -Destruction of information	-Modification of information -interception of information -Intrusion to the system -bribery
Terrorist	-Revenge -Blackmail -Design of institutions or government -Destruction	-Physical installations -Attaches to systems -Bomb -Penetration of the system -Management of the system -Information war
Spy	-Competitive advantage -Bio economic espionage	-Economic exploitation -Information theft -Penetration to the system -Access to classified information
Malicious contributors	-Revenge -Economic Retribution -Ego	-Commerce of sensitive information -Sale of personal information

As can be seen in the description of human threats, the actions that can occur for various reasons in a system of popular election may be accepting bribes, lack of technical training, curiosity, blackmail or threats by interested parties to change or object the results, the breach of security policies, or perhaps the most common is that employees do not fully comply with their work.

E. Controls

The purpose is to reduce the likelihood of a threat evidencing a vulnerability. The controls can be physical, technical and administrative:

Physical Controls

- Closed circuit cameras and monitors by area
- Private guards
- Inviolable identification of collaborators
- High power electric generator

Technical Controls

- Access control lists (ACLs)
- Intruder prevention systems in the network
- Disabling unnecessary services from servers and terminal equipment.
- DOS equipment attack detectors
- Storage of critical encrypted information

Administrative Controls

- Planning of actions in disasters
- Carry out emergency drills
- Registration of all personal data of collaborators
- Signing of confidentiality agreements with collaborators.
- Establish and make known internal regulations, information management policies and others to collaborators.

F. The probabilities

The probability that a threat will affect a system of popular election can be measured based on the following factors:

- Motivation of the threat
- Nature of vulnerability
- Effectiveness of controls

To obtain this measurement a qualitative scale of probability is applied:

1) High Degree: The threat source is well motivated and has sufficient capacity for action, the controls are not effective.

2) Medium Grade: The source of threat is motivated, has sufficient capacity for action, but the controls can be efficient.

3) Low Degree: It has no capacity for action or controls can prevent or reduce the chances of occurrence [6].

The analysis of the probabilities is carried out according to the source of the threats, which has been revised in previous lines:

TABLE II. PROBABILITY OF OCCURRENCE WITH HUMAN THREATS

Vulnerability	Threat	Control	Probability
Contributors accept bribes	Computational Criminal Spies Malicious staff	Security politics Rules of Procedure Criminal sanctions	High
Collaborators without technical training	Negligent contributors	Hiring collaborators with appropriate profiles and Training	Low
Collaborators without training On computer and electoral crimes	Hacker, Cracker Computer Criminal	Training collaborators on cyber and electoral crimes	Low

G. Impact analysis

This analysis consists of projecting the magnitude of the damage when a threat exploits a vulnerability, to evaluate it the criteria will be applied:

- Loss of Integrity (PI)
- Loss of Availability (PD)
- Loss of Confidentiality (PC)

Likewise, a qualitative scale will be applied:

1) High Degree: When three characteristics of information security are compromised.

2) Medium Degree: When two information security features are compromised.

3) Low degree: When an information security feature is compromised.

The impact analysis is also carried out according to the type of threat source: Human, Natural or Environmental [6].

TABLE III. IMPACT OF HUMAN THREATS

Vulnerability	Threat	PI	PD	PC	Impact
Contributors accept bribes	Computational Criminal Spies Malicious staff	**X**	**X**	**X**	High
Collaborators without technical training	Negligent contributors	**X**	**X**	**X**	High
Collaborators without training On computer and electoral crimes	Hacker, Cracker Computer Criminal	**X**		**X**	Half

III. RESULTS

A. Analysis of the level of risk

To assess the level of risk in the popular election system, the results of the probability and impact analysis of the previously analyzed threats are considered and a quantitative scale is given to the qualitative scale used in the previous measurements, this results in the following matrix:

TABLE IV. RISK LEVEL ANALYSIS

Probability Threat	Low Impact 10	Half Impact 50	High Impact 100
High 1.0	1.0 x 10 = 10	1.0 x 50 = 50	1.0 x 100 = 100
Half 0.5	0.5 x 10 = 5	0.5 x 50 = 25	0.5 x 100 = 50
Low 0.1	0.1 x 10 = 1	0.1 x 50 = 5	0.1 x 100 = 10

In this way, we obtain risk levels and their values, which is nothing more than the result of the multiplication between probability and impact when a threat exploits a vulnerability, resulting in the following risk levels [6]:

TABLE V. RANGE OF VALUES

level	Rank of Values
Low risk	1 - 5
Half risk	10 - 25
High risk	50 - 100

With this information, the risk for a system of popular elections can be assessed always according to the type of threat. We will use the criteria of the previous analyzes:

Probability (P): High (1.0), Medium (0.5) and Low (0.1)

Impact (I): High (100), Medium (50) and Low (10)

This assessment will give us the value of the impact and its respective classification.

TABLE VI. RISK EVALUATION FOR HUMAN THREATS

Vulnerability	Threat	P	I	Risk	
Contributors accept bribes	Computational Criminal Spies Malicious staff	**1.0**	**100**	**100**	**High**
Collaborators without technical training	Negligent contributors	**0.1**	**100**	**10**	**Half**
Collaborators without training On computer and electoral crimes	Hacker, Cracker Computer Criminal	**0.1**	**50**	**5**	**Low**

B. *Mathematical formula to calculate the risk in the model*

The following formula is used to calculate the risk between the probability and impact matrices:

$$P = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} I = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad (1)$$

$$R = P * I$$

R= Risk

P= Probability

I= Impact

C. *The risks of the system*

The analysis of risks according to the National Institute of standards and Technology NIST SP 800-30 indicates that systems in general are highly vulnerable to threats of human origin, the highest risks are the threat of computer criminals or malicious collaborators, because they can accept bribes, or be blackmailed and threatened. To reduce the risks, the following personnel hiring protocol can be established, which is the responsibility of the CNE. In addition to the selection process, emphasis should be placed on the process of verification of data and documents, verifying that they do not have political affiliation.

Next, a description of the protocol for each stage "Fig. 1":

- Reception of people to hire:

  From the selection made analyze and interview, collect documentation.

- 2.0 Document integration:

  Review and verification of information, filiation of the person.

- 3.0 Account management in banks:

  The account data to the banks for the payment process.

- 4.0 It is addressed to the functions that the profile adapts:

  The staff is directed to the coordinator of the venue or of meetings, data entry or others.

- 5.0 Formalities are carried out:

  Signature of contracts confidentiality clause

- 6.0 Training:

  Training according to your position

- 7.0 designation of places:

  Assignment of precinct zone or electoral boards

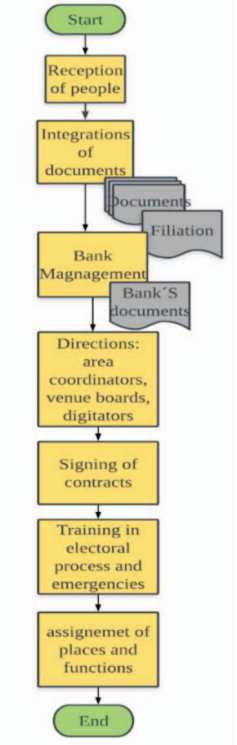

Fig. 1. Hiring process

As for threats of natural or environmental origin such as landslides, land subsidence and floods caused by heavy rains, disorganized mining and erosion of the land and those caused by poor infrastructure and other threats, they are low and susceptible to prevention in coordination with local institutions [4].

IV. DISCUSSION

If the risk levels are very high, it is necessary that immediate corrective measures are taken, the popular election system can continue to work, but the plan with the corrective actions must be implemented immediately.

If the risk levels are observed as means and corrective actions are needed, the plan must be developed within a reasonable timeframe.

If the observations determine that the risk is very low, it can be evaluated to take corrective actions or accept the risk.

The human being is the one that causes the highest risks, establishing a rigid personnel selection protocol could minimize the risks. These processes are structured with the use of standards, norms, protocols and methodologies to mitigate and minimize the risks associated with the technological infrastructure [8]. It is necessary that the electoral bodies make an effort to ensure that the system is reliable [14].

V. FUTURE WORK AND CONCLUSIONS

Definition of all the processes that involve electoral management; analyze as an alternative the implementation of a security protocol model for the STPR for the CNE, with the objective of reducing the risks in the integrity of the information of an electoral process.

The greatest risk is in the collaborators, their selection and hiring should not have a relationship in the policy, that meet a professional profile according to the functions or tasks they will fulfill and that demonstrate values such as honesty and ethics. There are electoral infractions that obtain sanction in the laws of the republic and criminal offenses must be denounced and sanctioned with the maximum rigor of the law, to establish precedents and minimize this risk.

ACKNOWLEDGMENT

The authors thank to Universidad Politécnica Salesiana del Ecuador, to the research group of the Guayaquil Headquarters “Computing, Security and Information Technology for a Globalized World” (CSITGW) created according to resolution 142-06-2017-07-19 and Secretaría de Educación Superior Ciencia, Tecnología e Innovación (Senescyt).

REFERENCES

[1] V. Manuel and M. Rocha, "Threats and vulnerabilities of remote electronic voting systems," vol. 13, pp. 119-136, 1994.

[2] E. Envelope, Organic Electoral Law, Code of Democracy. 2018

[3] CNE, "CNE performs sealing and zeroing of the transmission system and publication of results," CNE Sala press Not., 2019.

[4] L. of digital security and privacy of the K. Foundation (KLAB), "Proposed Audit Protocol for scrutiny of the elections of Colombia in 2018," 2018.

[5] NIST, " Guía para realizar evaluaciones de riesgo SP800-30rev1," NIST Spec. Publ. 800-30 Revis. 1, no. September, p. 95, 2012.

[6] Office of security for computer networks, "Methodology for the management of computer security (Project)," pp. 1-68, 2013.

[7] AG Oliva and EP Belleboni, "Methodology for the identification {{} {or} {}} of risks in voting systems {{} {ó} {}} n electr {{} {ó} {}} Nica, "Elections, vol. 13, no. 14, pp. 31-55, 2014.

[8] S. Francisco, E. Edgar, and B. Mirian, "Methodology of analysis and evaluation of risks applied to computer security and information under ISO / 27001," Rev. Tecnológica ESPOL, vol. 28, no. 5, 2015.

[9] A. Weitzenfeld, "Recent models of software process," Ing. Softw. object-oriented with UML, Java and Internet, pp. 54-56, 2005.

[10] OAS, "Technologies applied to the electoral cycle," Dep. For the Coop. and Obs. Elect., 2014.

[11] National Assembly, "Organic Electoral Law," 2009.

[12] M. D. E. L. A. Junta et al., "PRESIDENTA Msc. Ana Marcela Paredes Encalada Ing. Paúl Salazar Vargas Lcda. Luz Haro Guanga. "

[13] "ISO Standards," ISO / IEC15504 SPICE .

[14] M. Augusto and C. Espinoza, "Electronic voting: some lessons learned before and after its application in 2014 ERM," vol. 13, pp. 29-48, 2014.