Mitigating the Security of the Database by Applying a Conceptual Model of Integrity for the Civil Registry of Ecuador

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

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

José Antonio Orizaga Trejo
Department Information Systems
Centro U. Ciencias Económico Administrativas (CUCEA)
Guadalajara, México
jose.orizaga@academicos.udg.mx

***Abstract*—The confidentiality, integrity and availability of the information of the Civil Registry database of Ecuador were analyzed considering their functions, attributions and competences to determine why their priority is to mitigate the integrity of their data. The objective is to develop a prototype of a conceptual model of integrity to mitigate the security of the database and information. The deductive method was used to analyze the information of articles related to the research topic. Turned out a prototype of an integrity conceptual model to mitigate the inadequate modifications of Ecuador's Civil Registry data. It was concluded: That confidentiality, integrity and availability are important for information security but according to the mission, vision, strategic objectives of the Civil Registry of Ecuador has priority in ensuring the integrity of the database with a conceptual model appropriate. That the prototype to determine the risk value developed, defines the level risks of each of the civil acts of the people. The Prototype to mitigate the security of the database applying a conceptual model of integrity for the Civil Registry of Ecuador that was developed is an alternative to mitigate the security of the data and information.**

I. INTRODUCTION

Public and private organizations worldwide seek alternatives according to their environment to mitigate the security of information in their databases. The Civil Registry of Ecuador for its inconsistency that was determined in the database [1], requires defining an alternative such as mitigating the security of information; considering that the integrity of a database has priority according to the mission, vision, strategic objectives of the organization; which in this case study is to provide information with integrity of the civil acts of people national foreign migrants residing in Ecuadorian territory.

The security problems of Ecuador's Civil Registry database have been identified in the articles [1] [2]. The inconsistency of the data and information that has the Civil Registry in theirs database that is ratified by various means of communication of the written and spoken press, and the politicians of the Ecuador.

Why is it necessary to mitigate the risks and possible damages to the information, applying a conceptual model of integrity for the database of the Civil Registry of Ecuador?

For mitigate the security of the database with a conceptual model of integrity based on the mission of the organization for the delivery of the information of the civil acts of the people.

The objective is to develop a prototype to mitigate the security of the database applying a conceptual model of integrity for the Civil Registry of Ecuador.

The deductive method is used to analyze the information of articles related to the research topic.

The result obtained in this phase are:

That the authors considered the importance and priority of the integrity of the data and information supported in different schemes that are defined in the references noted in this article.

A prototype to determine the risk value of the Civil Acts of People, Threats, Frequency (F), Impact (I), Value of Risk (VR).

It is obtained the prototype conceptual model of integrity. This model allows to mitigate the inadequate modifications of the data or information of the database of the Civil Registry of Ecuador; this will allow evaluation in the application with the following mechanisms: Data elements, procedures, access control and integrity rules.

It was concluded:

- That confidentiality, integrity and availability are important for information security but according to the mission, vision, strategic objectives of the Civil Registry of Ecuador has priority in ensuring the integrity of the database with a conceptual model appropriate.
- That the prototype to determine the risk value developed, defines the level risks of each of the civil acts of the people.

- The prototype to mitigate the security of the database applying a conceptual model of integrity for the Civil Registry of Ecuador that was developed is an alternative to mitigate the security of the data and information.

II. MATERIAL AND METHODS

In the first instance we considered the information of the published articles with direct relation to the research topic "Algorithms and security protocols for the Civil Registry of Ecuador". Several articles related to the topic.

Materials

We analyzed in this phase the articles that have relation with the subject of investigation:

The author states that the hiring of the service for the integrity of the data to an alternates companies is a valid option; provided for the analysis of the different models that the organization has to mitigate the integrity of the data; indicates that is prohibits privileges and rights to the service provider so that you can update data[3]. Defines the different rules for data integrity in a relational database; considers a new method to consolidate the integrity of data by groups using an infinite state machine with the language in the MS SQL Server DBMS[4]. To solve the problems of integrity levels we consider the use of different platforms that work in a distributed architecture; constructs a prototype based on questions of models, architecture and policies that the organization disposes[5]. The subcontracting of signatures that guarantee the integrity of the data; in this case they developed three new schemes called practical and immutable signature bouquets (PISB); (i) Condensed-RSA (C-RSA) and Sequential Aggregate RSA (SA-RSA) based scheme called PISB-CSA-RSA, (ii) a generic scheme called PISB-Generic, and (iii) a scheme that enables efficient immutable aggregate signature pre-computation called PISB-RP[6]. The author is based on the application of code generated in a programming language to guarantee the integrity; considers two proposals: The first is the technique to avoid compromised or falsified code and the second is based on analyzing mechanisms designed to mitigate the effects of malicious codes; in addition to analyzing some techniques to ensure the integrity and reliability of certain applications such as executable file integrity, digital signatures, reliable computing[7]. Integrity as a service in the cloud does not guarantee; while the servers are not owned by the organization; it is important to perform an analysis of the architecture of the subcontracted database; the author consider in analyzing authenticated based method, probabilistic based method; the author's approach is to generate a mechanism to create fake tuples to insert in the subcontracted database; using two functions to create attributes: Periodic input and generation function[8]. This Clark-Wilson model is used to protect the integrity of the information of commercial companies; for this reason on this occasion make the modification in the mechanical access control consisting of; in using the integrity level as the basis for object modification; is adopted to configure user access control with TP (Transaction Procedures), IVP (Integrity Verification), CDI (Restricted), UDI (Unrestricted), defines three rules, also considers access control[9]. Integrity-based security usually depends on a third party in which they trust the data; this paper proposes the virtual distributed agent model of the machine, and the model provides a unique solution through virtual machine monitoring for each user in the cloud[10]. The integrity of the information in a web page is very important in view that a security violation in a webpage affects to the Verena servers where are the clients that can verify the integrity of a web server; the concepts Verena and Api can be observed the examples of the execution in remote monitoring medical application, trust contexts, integrity query prototypes, queries API, querying across trust contexts, deriving trust contexts from user input, integrity guarantees. Also consider la integrity protection mechanism based in ADS forest, completeness chain implementation, IQP analyzer, trust context membership operations[11].

Methods

The deductive method was considered to analyze the information available on scientific articles related to the topic. In the first instance, the articles published with direct relation to the research project "Algorithms and security protocols for the civil registry of Ecuador" were revised; in which are defined the problems of the security of the database of the Civil Registry of Ecuador.

Processes executed

1) A scale was defined to measure the frequency and impact on the integrity of the information in a range of 0 to 5 based on the Function Points Analysis Training Course[12].

TABLE I. SCALE TO MEASURE THE FREQUENCY AND IMPACT OF INFORMATION INTEGRITY

Rating Frequencies (F)	Interpretation Impact (I)	Score
Never	Not present, or no influence	0
Hardly ever	Incidental influence	1
Sometimes	Moderate influence	2
Often	Average influence	3
Usually	Significant influence	4
Always	Strong influence throughout	5

2) The most frequent potential threats and vulnerabilities that *Record of Facts and Acts Relating to the Civil Status of Persons*. The General Directorate of Civil Registry, Identification and Registration shall solemnize, authorize, register and record, among others, the facts and acts related to the civil status of the persons and their modifications that are 27 but that for the purpose of methodology are described below 10 acts civilians of the people[13].

TABLE II. POTENTIAL THREATS AND VULNERABILITIES IN THE INTEGRITY OF INFORMATION

Civil acts of persons	Intentional Threats	Vulnerabilities
Data Integrity / Information		
Births	Do not record the actual date, professional players with false ages	Lack of control in hospitals, family, geographic location
Changes, additions and	Incorrect identity	Unauthorized persons

Civil acts of persons	Intentional Threats	Vulnerabilities
deletions of names		for registration
Changes and notary possessions of surname	Access to inheritances or economic actions	Notaries are not yet linked to the civil registry
Adoptions	Trafficking of newborns	Procedures without legal support that are registered in real time in the database of R.C.
Recognition of sons and daughters	Late registration not recognized by biological parents	Do not have direct links to the database from hospitals or clinics
The marriages	People with N marriages	Lack of verification of documents in internationally secure systems
The divorce	That a person without having been legally notified of this divorce	Database without integrity allows unauthorized persons to perform this act
The union in fact	That the de facto union is not legal and valid	Registration in any notary who does not have an information security certification
Deaths	Dead who are still voting	Lack of control in the online records in the database
The disability status of people	Collection of compensation that does not apply	Professionals who grant this condition and do not register in real time in the database

3) A general scheme was identified as an alternative to define future security policies and mechanisms for database integrity based on references: BLP Model, Biba Model, Clark-Wilson Model[14]. In this investigation the priority is to define a prototype to protect the integrity of the database and information of the Civil Registry of Ecuador.

TABLE III. LEVELS TO MITIGATE INTEGRITY OF THE DATABASE

Levels	Security politics	Mechanisms of control
Top secret	The policies to be defined in the future should be oriented at all levels. These can be for physical security, administrative logic, database, among others	For each security policy, a minimum control mechanism must be generated; Recommended three for each policy
Secret		
Confidential		
Not classified		

The Table III. Defines a scheme of security policies and mechanisms that should be considered for the application to classified information of the Civil Registry to mitigate the integrity of data.

III. RESULTS

After performing the exploratory research in this phase the following results are obtained.

1) The authors consider the importance and priority of the integrity of the data and information supported in different schemes that are defined in the references noted in this article.

2) A prototype to determine the risk value of the Civil Acts of People, Threats, Frequency (F), Impact (I), Value of Risk (VR).

TABLE IV. PROTOTYPE TO DETERMINE THE RISK VALUE

Ord	Civil act of the people	Threat	F	I	VR
1	Births	Do not record the actual date, professional players with false ages	3	5	15
2	Changes, additions and deletions of names	Incorrect identity	2	5	10
3	Changes and notary possessions of surname	Access to inheritances or economic actions	2	3	6
4	Adoptions	Trafficking of newborns	1	4	4
5	Recognition of sons and daughters	Late registration not recognized by biological parents	2	5	10
6	The marriages	People with N marriages	2	3	6
7	The divorce	That a person without having been legally notified of this divorce	3	3	9
8	The union in fact	That the de facto union is not legal and valid	2	3	6
9	Deaths	Dead who are still voting	2	5	10
10	The disability status of people	Collection of compensation that does not apply	2	2	4

In Table IV. The scale is applied to measure the frequency and impact of the integrity of the information to obtain the risk value that in no case will be greater than 25 with the application of the scale of Table I.

Interpretation of the value of risk (VR):
if F×I≥0 and ≤ 3=0
if F×I>3 and ≤6=1
if F×I>6 and ≤9=2
if F×I≥10 and ≤15=3
if F×I≥16 and ≤20=4
if F×I>20 and≤25=5

The values that are obtained in the prototype of the risk value (VR) that its result is ≥9; will be those that must be implemented controls with policies and security mechanism, to mitigate the integrity of the data.

3) We obtained the prototype conceptual model of integrity.

This model allows to mitigate the inadequate modifications of the data or information of the database of the Civil Registry of Ecuador; this will allow evaluation in the application with the following mechanisms: data elements, procedures, access control and integrity rules; to elaborate this prototype was considered the references of the model of Clark Wilson[9].

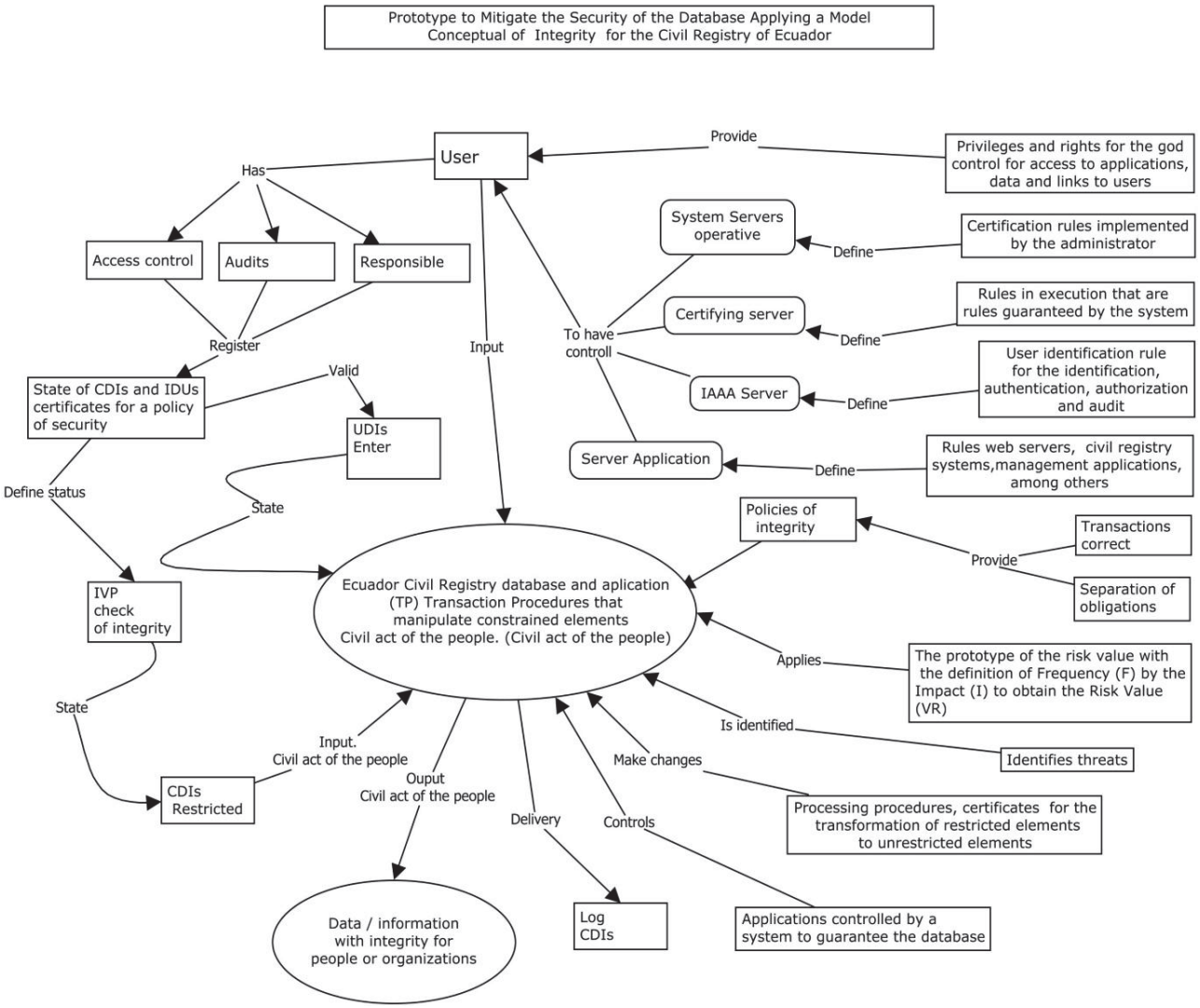

Fig. 1. Prototype of a conceptual model of integrity with the actors involved

Prototype Overview:

The user has:

- Control of accesses, audits, responsible
- Privileges and rights
- Control through operating system servers, certifying server, IAAA server, application server.

The database must have:

- Integrity policies
- The prototype of the risk value is applied
- Identifies Threats
- Change can be made through transformation procedures, certificates for the transformation of restricted elements to unrestricted elements.
- Applications controlled by a system to guarantee the database.
- Delivery log CDIs
- Delivery of data and information with integrity for the persons or organizations of the Civil Acts of the people who live within the Ecuadorian territory.
- It must be controlled by the restricted CDIs through the IVP (integrity check).
- Validate IDUs for income

The prototype to mitigate the security of the database applying an integrity conceptual model for the Civil Registry of Ecuador defined in Fig. 1. allows a visualization of the main actors in this case study that must intervene to mitigate the security of the database with the use of an integrity model.

Prerequisites for implementing a prototype of the integrity conceptual model in an organization or institution:

Preliminary information:

- Carry out the analysis of the mission, vision, strategic objectives for which the institution or organization was created.
- Evaluation of available hardware and software
- The structure or configuration of the middleware, corba, DBMS.
- Which operating systems you have under a distributed architecture.
- Developed applications available for management
- Application software
- Software and hardware available for the management of information security such as (Firewall, encryption software, digital signatures, among others).
- Consider the safety standards ISO 177799, ISO 27001, among others.

How to determine the state of information security in the organization:

- Conduct an analysis of the organization's processes
- Risk analysis of vulnerabilities and threats
- Develop a risk value
- Determine how often threats and risks are run
- The impact of threats
- Define security policies at a physical and logical level
- Define mechanisms for compliance with information security policies.

With the results obtained from the previous work detailed above, the prototype was developed to mitigate the security of the database applying a conceptual model of integrity for the Civil Registry of Ecuador.

The contribution in this investigation is the development of the prototype of the conceptual model of integrity for the Civil Registry of Ecuador; with the integration of privileges, user rights, controls through operating system servers, security certifiers, IAAA, application server among others; anticipated the fulfillment of the prerequisites to implement a prototype of the conceptual model of integrity.

IV. DISCUSION

The results obtained in this phase are: The authors' criteria regarding the integrity of the database and information that determine the priority with relation confidentiality and availability. A prototype of the risk value of the civil acts of the people with their respective threats, frequencies, impact to obtain of the value of the risk and the prototype of a conceptual model of integrity was obtained to mitigate the inadequate modifications of the database of the Civil Registry of Ecuador.

In this research the problem of data integrity is not solved but a prototype of a conceptual model of integrity is obtained; as an alternative to mitigate safety.

The authors of the revised articles consider integrity of data and information to be a priority with relation confidentiality and availability; but none exposes a conceptual model of integrity to mitigate the security of the database and information without relying a specific technology infrastructure.

This prototype of the integrity conceptual model can be taken as reference for applying in organizations, public or private institutions worldwide. With the analysis of the requirements defined for implementation in this article prior to application. The Civil Registry of Ecuador will have as an alternative for the short term application.

The following was concluded:

1) That confidentiality, integrity and availability are important to mitigate the security of information; but according to the mission, vision, strategic objectives of the Civil Registry of Ecuador its priority is to ensure the integrity of the information with an appropriate conceptual model.
2) The prototype of the risks value that was obtained on the civil acts of the people who live in the Ecuadorian territory; have threats with a frequency that is based on type of civil act that will have an impact the same that were qualified based on Table I. to obtain the risk value; its mitigation is recommended from a rating greater than nine; it should be considered that the highest rating it can reach is 25 based on Table I.
3) The Prototype to Mitigate Database Security Applying an Integrity Conceptual Model for the Civil Registry of Ecuador was developed with the globalization of information security management at a technical, administrative, operational, tactical and strategic level that will allow to mitigate database integrity.

From the conclusions performed is sustenance:

1) With regard to the first conclusion, we agree that data integrity takes precedence over confidentiality and availability depending on the mission, vision and strategic objectives of the organization; we support the different authors who support this thesis according to the reference of the revised articles of the [3-11].
2) To carry out the prototype of the risk value, the safety standards ISO 177799 and 27001 were taken as a reference, generating the frequencies, impact and risk value; the rating method is based on Function Points Analysis Training Course [12].
3) To develop the prototype to mitigate the security of the database applying a conceptual model of integrity for the Civil Registry of Ecuador it is base the article [1] and, [2] in which an identity management model was generated applying the IAAA in order to mitigate information security without relying on specific technology infrastructure. He Clark-Wilson article describing the integrity of the data was considered for the development of the conceptual model of integrity [9], which is oriented to the integrity of data and information for commercial companies and finally considered the articles of reference [3-11].

V. Future works and conclusion

Develop a conceptual model of integrity appropriate to the Civil Registry of Ecuador; considering the 27 processes that it performs for its management; based on its mission, vision and short-term strategic objectives.

Conclusions:

- That confidentiality, integrity and availability are important for information security but according to the mission, vision, strategic objectives of the Civil Registry of Ecuador has priority in ensuring the integrity of the database with a conceptual model appropriate.
- That the prototype to determine the risk value developed, defines the level risks of each of the civil acts of the people.
- The prototype to mitigate the security of the database applying a conceptual model of integrity for the Civil Registry of Ecuador that was developed is an alternative to mitigate the security of the data and information.

Acknowledgment

The authors thank CUCEA of Universidad de Guadalajara, Jalisco, México, Program IT PhD Information Technologies, Universidad Politécnica Salesiana del Ecuador and Secretaria de Educación Superior Ciencia, Tecnología e Innovación (Senescyt).

References

[1] P. D. Student, S. Moisés, T. Toapanta, P. D. Luis, and E. Mafla, "Security analysis of civil registry database of Ecuador," *Int. Conf. Electr. Electron. Optim. Tech. - 2016*, pp. 1024–1029, 2016.

[2] P. Segundo, M. Toapanta, P. D. Luis, and E. Mafla, "Analysis to define management of identities access control of security processes for the registration civil from Ecuador," in *2016 IEEE International Smart Cities Conference (ISC2)*, 2016, pp. 80–84.

[3] D. W. L. Cheung, "Security and integrity in outsourcing of data mining," *2008 IEEE Int. Conf. Granul. Comput.*, no. i, p. 2007, 2008.

[4] A. Malikov, V. Voronkin, and N. Shiryaev, "Models of integrity assurance in big relational databases," *Proc. - 2016 10th Int. Conf. Qual. Inf. Commun. Technol. QUATIC 2016*, pp. 179–184, 2017.

[5] C. Jenkins and L. Pierson, "Integrity levels: A new paradigm for protecting computing systems," *Proc. - 2014 IEEE 13th Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2014*, pp. 534–543, 2015.

[6] A. Yavuz, "Immutable Authentication and Integrity Schemes for Outsourced Databases," *IEEE Trans. Dependable Secur. Comput.*, pp. 1–1, 2016.

[7] L. Catuogno and C. Galdi, "Ensuring Application Integrity: A Survey on Techniques and Tools," *Proc. - 2015 9th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS 2015*, pp. 192–199, 2015.

[8] P. Ghazizadeh, R. Mukkamala, and S. Olariu, "Data integrity evaluation in cloud database-as-a-service," *Proc. - 2013 IEEE 9th World Congr. Serv. Serv. 2013*, pp. 280–285, 2013.

[9] Q. Xu and G. Liu, "Configuring Clark-Wilson integrity model to enforce flexible protection," *CIS 2009 - 2009 Int. Conf. Comput. Intell. Secur.*, vol. 2, no. 1, pp. 15–20, 2009.

[10] X. Xu, G. Liu, and J. Zhu, "Cloud Data Security and Integrity Protection Model Based on Distributed Virtual Machine Agents," *2016 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov.*, pp. 6–13, 2016.

[11] N. Karapanos, A. Filios, R. A. Popa, and S. Capkun, "Verena: End-to-End Integrity Protection for Web Applications," *Proc. - 2016 IEEE Symp. Secur. Privacy, SP 2016*, pp. 895–913, 2016.

[12] D. Longstreet, "Function Points Analysis Training Course," *Longstreet Consult. Inc. Acessed*, vol. 2, p. 15, 2005.

[13] R. O. S. De, H. Del, P. Barrezueta, D. E. L. E. Y. Organica, D. E. G. D. E. La, and I. Y. Datos, "DATOS CIVILES," Quito, 2016.

[14] J. Jin and M. Shen, "Analysis of Security Models Based on Multilevel Security Policy," *Manag. e-Commerce e-Government (ICMeCG), 2012 Int. Conf.*, pp. 95–97, 2012.