The “Delegate of Data Protection”: Strategic Planning in information security Case Ecuador

Tannia Cecilia Mayorga Jácome 1, Joe Luis Carrión Jumbo 2, Álvaro Gabriel Benítez Bravo 3 and Henry Rodrigo Vivanco Herrera 4

1 Universidad Tecnológica Israel, Ecuador - Quito, Francisco Pizarro E4-142 y Marieta de Veintimilla, 2 Universidad Internacional SEK, Ecuador - Quito, Carcelén, 3 Universidad Técnica particular de Loja, Ecuador – Loja San Cayetano Alto, Calle Paris, 4 Universidad Iberoamericana del Ecuador - Quito, 9 De Octubre N25-12 y Av. Colón Esq.

Abstract. Information security over time has been taking important scenarios in the world, along with regulations and laws have had to adapt to this evolution in such a way that protection, compliance, and sanctions are guaranteed. A sample of this is the new European Data Protection Regulation in force since May 25, 2018, where it administers the function of "Data Protection Delegate" (DPD) or Data Protection Officer (DOP). Since this position is new to the rest of the world, concerns arise about the functions that it will have to fulfill in Latin American countries, where most of them already have a Data Protection Law but not with the position of Delegate as such. This study aims to justify the need for this new position, through a SOWA analysis of PESTEL, compilation of reports, interested stakeholders of the project, in addition to publicizing the guidelines, roles, fields of action, risk prevention and audit in terms of compliance.

1. Introduction

1.1 Approach of the work

Currently, from the business management, there is a latent requirement to adopt in the information and communication systems referring to the increasingly specific and imminent need of business strategies according to their business (Core Business).

The real problem in security issues in information technology and communication is that cyber-attacks do not know the limits between countries, but on the contrary, they act in the world, violating all types of security with the sole purpose of obtaining the information they require, regardless of the damage they cause to third parties. That is the reason for this research, to raise awareness of the need for strategic planning where the need for the “General Data Protection Regulation (GDPR)” [1] [2] like in Europe and the Data protection delegate (DPD) is evident not only in Europe but also in Latin America.

Fundamental proof of this has been the events of recent years such as the Wannacry ransomware (WanaCryp0r 2.0), the same one that affected many telecommunications providers (trail one, carrier,
ISP, among others). even more than 150 countries were affected, which set off all cybersecurity alarms [3]. Likewise, on September 16, 2019, 18 GB of personal data of Ecuadorians were violated due to a serious computer failure. [4]

At the legal level in numeral 19 of article 66 [5] it states as a right pre-assumed to personal data protection both the data and the information of an individual; likewise, article 92 of the Constitution of the Republic of Ecuador [5] regarding habeas data indicates documents, genetic data, banks or personal data files as protection assumptions.

On the other hand, it is important to indicate that in Ecuador the Data Protection Law was discussed by the Assembly in the first debate on February 2 and 3, 2021. The second debate on May 10, 2021, and has just been approved on 21 May 2021 by outgoing President Lennin Moreno (National Assembly of Ecuador, 2021)[6].

1.2  Evolution and prospective towards a strategic and integral concept of the Delegate of Data Protection

Due to the lack of knowledge of compliance issues to manage information security management, there are currently several standards among them: ISO 31000 and ISO 27001, ISO 20000, which in 2000 were seen as something distant and currently are a reality in favor of continuous improvement (cycle of Deming PDCA) to evolve with the complement of methodologies for risk management, such as ISO 27005, ISO 31000, Magerit (PAE-Magerit, 2012) considering the type of method, its effectiveness, adaptation to the company and resources required.

A subject that is not very much addressed and that definitely in the prospective that is presented to the year 2050 is to talk about economics of information security that "provides valuable insights not just into security […] but into more general areas such as the design of peer-to-peer systems, the optimal balance of effort by programmers and testers, why privacy gets eroded, and the politics of digital rights management " [7], in Latin America and even more in Ecuador, but of high global importance, because it makes reference to the cost problem that implies having an adequate computer security within the companies, where the human, technological and legal capital are available. Sustain the operation and security of the company's data. As well as the costs that would imply the not having within the companies the aforementioned to invest after an attack on these issues of IT security. Everything that is preventive rather than reactive will always be better and therefore less expensive for companies, information is something very delicate in the daily operation at all levels. Therefore, it is necessary to manage different scenarios where even catastrophic events such as black swans are considered by companies [8] or to think about integrating anti-bribery policies as a result of comprehensive risk analysis; in such a way that the reliability, integrity, availability of the information can be met, not repudiation, granting flexibility, reliability and above all digital confidence to both the client and the employer.

1.3  Formulation of the problem

Is it necessary that there exist in Ecuador a data protection regulation and therefore the figure of Delegate of Data Protection?

1.4  Overall objective

Develop all the necessary evidence to justify the need for the Delegate of Data Protection in Ecuador in the business sector.

1.5  Specific objectives

- Identify potential stakeholders in data protection at the corporate level.
- Collect evidence that justifies the need for the Delegate of Data Protection.
2. Methodology
For the development of this article, a qualitative methodology was used through the application of bibliographic techniques and, a documentary from reports, regulations, and specialized authors. A PESTEL macroenvironmental analysis is proposed as a tool [9], which analyzes factors such as political, economic, social, and technological that justify the need to have a DPD; thus obtaining opportunities and threats, and then complementing them with an AMOFHIT analysis (microenvironment) taking into account important parameters such as: administration and management, marketing and sales, operations and logistics, finance and accounting, human resources, information systems and communication, technology, research and development. Product of the PESTEL analysis conjugation, with the AMOFHIT analysis we can have a comprehensive SWOT analysis [10] that "was proposed by the management consultant Albert S. Humprey, in the 70's in the country of the United States due to an investigation by the Stan-ford Research Institute that aimed to reveal the failure of the corporate organization" [11], in order to demonstrate that, as in the case of European Community the fact of having a GDPR and the figure of the DPD are equally necessary for Ecuador because as Martin says this data protection requires greater complexity in the regulations and is part of many disciplines [12].

3. Results
3.1 Functions of the Delegate of Data Protection
Based on the European Data Protection Regulation [13], you can see in figure 1 a summary of the functions of the DPD for which you will have to take charge, this graph was prepared with information from the Agency Spanish Regulation and Data Protection.

The profile of the professional who complies with these functions will require knowledge of the data protection regulations (see Figure 1)

Figure 1: Delegate of Data Protection and its functions
This information is a reference for the functions of the DPD for Ecuador, although it is necessary to consider the person in charge of security, and that role is assumed by the head of the technical department in the best of cases.

3.2 **PESTEL Analysis**

For the analysis of the macro environment, the following aspects are considered: political, social, technological, and legal so it would be a PSTL analysis which are detailed in Table 1:

| Opportunities                        | Threats                                      |
|--------------------------------------|----------------------------------------------|
| 1. Right to the protection of personal data. | 1. New forms of infringement |
| 2. Access to information             | 2. Files and data in the cloud               |
| 3. There is RGPD in Ecuador.         | 3. Absence of consent on private information of a subject |
| 4. The trend of companies is towards Digital | 4. Changing policy                        |

3.3 **AMOFHIT Analysis**

Table 2 shows the strengths and weaknesses of AMOFHIT (microenvironment) analysis [14].

| STRENGTHS                                      | WEAKNESSES                                      |
|-----------------------------------------------|-------------------------------------------------|
| 1. Right to privacy                           | 1. The informed consent of the person to his information is not regulated. |
| 2. Habeas Data fundamental right               | 2. Companies should invest in changes in their systems and a professional data protection delegate |
| 3. Ecuador has approved the data protection law. | 3. Lack of knowledge                             |
| 4. Companies need to protect them Data         | 4. Small and medium businesses still document their sensitive data on paper |

3.4 **SWOT Analysis**

Companies need to protect, considering the statement made by Ramírez Rojas: "The use of the SWOT analysis as a tool is not limited to large organizations or companies [...], on the contrary, its application should be promoted in micro and small companies to equip them with an adaptable instrument and efficient formal planning, in support of its administrative practices and improving its competitiveness" [15], it is necessary to make a microenvironmental analysis of strengths opportunities showed in Table 3.
Table 3. Analysis microenvironments strengths opportunities

| Offensive areas of strategic initiative relationship S-O: | S-O: | OPPORTUNITIES (Numbers of Table 1) |
|---------------------------------------------------------|------|-----------------------------------|
| Low: 1                                                  |      |                                   |
| Medium: 3                                               |      |                                   |
| High: 5                                                 |      |                                   |
| STRENGTHS (Numbers of Table 2)                          |      |                                   |

| Right to the Protection of personal data                | Access to information | Companies must make changes to adapt to the new law | The trend of companies is towards to digital | Total | Priorization |
|--------------------------------------------------------|-----------------------|----------------------------------------------------|-----------------------------------------------|-------|--------------|
| Right to privacy                                       | 5                     | 5                                                  | 3                                             | 3     | 16           | 2             |
| Habeas Data fundamental right                          | 5                     | 5                                                  | 3                                             | 1     | 14           | 1             |
| Ecuador has approved the data protection law           | 5                     | 3                                                  | 3                                             | 5     | 16           | 3             |
| Companies need to protect them Data                    | 5                     | 5                                                  | 5                                             | 5     | 20           | 4             |
| Total                                                  | 20                    | 18                                                 | 14                                            | 9     |               |               |
| Priorization                                           | 4                     | 3                                                  | 2                                             | 1     |               |               |

By analysing the microenvironment and performing the respective rates, can be verified that the most critical point to consider are Habeas Data fundamental right with changing policy.

Table 4 shows the relationship between threats and weaknesses, where the critical point is represented by the variables Companies should invest in changes in their systems and a professional data protection delegate.

Table 4. Macroevironmental analysis of weaknesses and threats

| Defensive areas of strategic initiative relationship W-T Low: 1 | THREATS (From Table 1) |
|---------------------------------------------------------------|------------------------|
| Medium: 3                                                      |                        |
| High: 5                                                        |                        |
| WEAKNESSES (From Table 2)                                     |                        |

| New forms of infringement | Files and data in the cloud | Absence of consent on private information of a subject | Changing policy | Total | Priorization |
|---------------------------|-----------------------------|--------------------------------------------------------|-----------------|-------|--------------|
| The informed consent of the person to his information is not regulated | 5 | 1 | 3 | 3 | 12 | 4 |
| Companies should invest in changes in their systems and a professional data protection delegate | 5 | 5 | 3 | 5 | 18 | 1 |
| Lack of knowledge         | 5 | 5 | 3 | 3 | 16 | 2 |
| Small and medium businesses still document their sensitive data on paper | 5 | 5 | 1 | 3 | 14 | 3 |
| TOTAL                     | 20 | 16 | 10 | 14 |       |               |
| PRIORIZATION              | 1 | 2 | 4 | 14 |       |               |

5
Table 5 shows a list of strengths and weaknesses where the cognitive area related to the crossing variables is prioritized giving a range of assessment to know what is the strength that seeks to correct the weakness to address the areas that show the weaknesses: legal, skills, technology, and security.

| Code | Item                                                                 | Defensive priorization | Strategic area |
|------|----------------------------------------------------------------------|------------------------|----------------|
| W1   | The informed consent of the person to his information is not regulated. | 1                      | Legal          |
| W2   | Lack of knowledge                                                    | 2                      | Competences    |
| W3   | Small and medium businesses still document their sensitive data on paper. | 3                      | Technology     |
| W4   | Companies should invest in changes in their systems and a professional data protection delegate | 4                      | Security       |
| S1   | Companies need to protect their data.                                 | 1                      | Security       |
| S2   | Ecuador has approved the data protection law                          | 5                      | Legal          |
| S3   | Right to privacy                                                     | 4                      | Security       |
| S4   | Habeas Data fundamental right.                                       | 2                      | Security       |

Table 6 shows an order of priority of the strategic areas that range from least to greatest to establish the order in which the strategies that constitute legal matters must first be executed, then knowledge, technology and then security; this in the offensive part.

| Offensive Priority | Strategic Area |
|-------------------|----------------|
| 1                 | Legal          |
| 2                 | Competences    |
| 3                 | Technology     |
| 4                 | Security       |

| Defensive Priority | Strategic Area |
|-------------------|----------------|
| 1                 | Security       |
| 2                 | Legal          |
| 3                 | Security       |
| 4                 | Security       |

In the defensive part of the strategy, it is also observed that there is a legal problem to start working on the data security factor.
In terms of security, the SWOT is necessary to know how to counteract the expected growth; for this, we take the mentioned trends on the global market and data protection in the cybersecurity cloud by Vasquez:

 [...] the 2016-2020 period is 9.5% annualized and for 2021 it is expected to reach 172,000 million euros, a figure especially important considering its short life.

In certain market segments, such as Security and Data Protection in the Cloud (SaaS) and Next-Generation Malware Detection, growth is expected to be significantly above the market, with annual growth rates (2014-2020) between 37% -50%. [16]

Several trends explain the rapid growth that the cybersecurity market is experiencing and the positive outlook for the next few years, then Table 7 shows the high interest that project managers have in managing the security of the information appropriately.

### Table 7. Interested stakeholders of the project

| Name of then interested | Role                   | Power  | Interest | Strategy                                    |
|-------------------------|------------------------|--------|----------|---------------------------------------------|
| Company Manager         | Sponsor                | High   | High     | Manage carefully                           |
| "Delegate Data protection" | Regulator              | Low    | Medium   | Monitor data                               |
| Financial delegate      | Financier              | Medium | High     | Non-repudiation of information             |
| Director of Development | Director of the system development area | High   | High     | Availability of information                |
| Administrative Director | Director of the administrative area of the project development, equipment sizing, graphic design | High   | High     | No repudiation of information              |
| Members of the technical team | Development,                      | Medium | High     | Security tools                             |
| Suppliers                | Provider                | Low    | Medium   | Keep informed                              |
| Marketing staff          | Seller                 | Low    | High     | Keep Satisfied                            |
| Business owners          | Final user              | Low    | Medium   | Keep informed                              |
| Business managers        | Final user              | Low    | Low      | Monitor slightly                          |
| Business Service Personnel | Final user              | Low    | Low      | Monitor slightly                          |

#### 3.5 Evidence collection

##### 3.5.1 Cyberattacks trends. Cyberattacks trends were collected from reports made by reliable sources such as Risk Based Security, IMAP International M & A Partners [17] where they show with many attacks of more than 5000 violations and 7.89 billion records exposed, the year 2017 marked a record in the number of violations, which 55% were caused by piracy. However, this was not the main reason why the records were exposed. The 5 main attacks exposed about 5.7 billion records; or what is the
same, 72% of the total of the records exposed during 2017. Additionally, there is mentioned “In the first trimester of 2019 there have been three breaches exposing 100 million or more records” [18]

It is also worth highlighting the report of International M & A Partners, the following: theft or exchange of cryptocurrencies with a value of 500,000,000 euros, the affectation of the WannaCry. Ransomware in 150 countries; Petya provoking the closing of large public Corporations, AP. Moller-Maersk's booking system paralyzed all cargo transport with an estimated cost of 300 million. [17]

In relation to the above, it can be indicated that the economic repercussion resulting from vulnerabilities referring to data is extremely high for the companies, which constitutes another evidence for the present study.

3.5.2 Cybersecurity series reports of CISCO. According to the report of OWASP - CISCO it is extracted as evidence: the increase of malware during November 2016 and October 2017 from 19% to 70%; the proliferation of ransomware worms. However on 2019 the ransomware has lost its throne because only a small percentage of victims pay the ransom, the growth of botnets (the same that are seen as threats only by 13% of organizations there is an increase in IOT devices without paying attention to security, there is greater complexity in Cyber-defense, they rely on solutions from several suppliers, which means that there is a greater reduction in the cyber-defense capacity of companies and, from the point of view of Spanish professionals, almost 50% indicate the complexity of this management and 74% specify this in security alerts. [19]

Concerning the highlight of OWASP - CISCO, there is evidence of the increase in Cybercrime, the intelligence in the propagation of malware, botnets becoming increasingly complex the control and management by the security managers, which incidence in the data protection directly.

In the CISCO privacy data report mentions: “The findings of this study provide solid evidence that organizations receive benefits additional to compliance by their investments in privacy” [20]. Interesting contribution considering that the population of the entire world surveyed was not only from member countries of the European Union.

3.6 Data breaches

The information showed in Avast blog [21] of the top 10 data breaches total 1270 million people affected, highlighting the impressive information of people affected; and the vulnerabilities to which people are prone and how delicate it is to store information such as credit cards; that could front legal consequences Reputational and financial impact on customers [22]

It is notorious that some companies invest little in cybersecurity and data protection, which evidences the need for the data protection delegate at all levels.

4. Discussion

After summarizing the criteria considered to justify the role of data protection delegate in Table 8, it can be deduced that companies must take action on the matter so that there is a DPD within their payroll, which constitutes a figure with important functions and responsibilities, which does not necessarily have to be a lawyer, but a person who have knowledge of information security to handle or know issues such as: legal and regulatory aspects in data security, risk management under ISO 31000, ISO 25000, IT service management ISO 20000, information security under ISO 27001, CISO (Chief Information Security Officer) security audit.
Table 8. Summary of criteria to justify the role of "Delegate of Data Protection"

| Criterio                                      | Analysis                                                                 |
|-----------------------------------------------|--------------------------------------------------------------------------|
| SOWA                                         | Analysis of the environment and reality of Ecuador in terms of information security and data protection, considering four fundamental axes on which the matrix is based. After the analysis carried out and based on what the theories worked by different authors say, it can be concluded that data security is a factor of great importance for companies in the globalized world. |
| Possible interested                          | Worldwide there are interested in managing security as sponsors, regulators, financiers, systems development area directors, project management area directors |
| Evidence collection                          | Evidence of Cisco Series reports, International M & A Partners, Avast, "Data protection" Group Article 29 and Attacks made to the data; The companies that were susceptible to attacks whose involvement involved millions of people belong to the private sector, so it is not enough that a "Data Protection Delegate" is only available to public companies as indicated in the preliminary draft presented by DINARDAP. |
| Rules of support for the "Delegate of Data Protection" | ISO 27001, ISO 31000, ISO 25000, ISO 20000 |
| Functions of the "Delegate of Data Protection" | Since, in Ecuador, in most companies, there is no security officer, the "Data Protection Delegate" should also assume this role, so that knowledge and preparation in security area will be important, as a digital right. |

The European Regulation already has a long history, that is why it can separate the functions of the DPD and Head of Information Security [23], in Ecuador a developing country, it would possibly have to assume both functions in medium and small companies, since the IT manager generally has to achieve multiple roles.

This reality added to what Wang says, "Technology evolves before the Laws", surely as this new law is implemented in the public and private sector, further adjustments are required [24]. On the other hand, the large amount of data that is generated by IOT devices must be taken seriously since the privacy of the information is especially important as well as the protection of personal data [25]. That is why models are designed to guarantee the security of information [26].

5. Conclusions

Data protection impact evaluations are a useful way for decision-makers to apply data processing systems that comply with the General Data Protection Regulation of the European Union and may be required to certain types of treatment operations, which can be adopted in Ecuador.

The person responsible for the treatment will apply technical appropriated measurements to guarantee and be able to demonstrate this treatment.

Therefore, it can be deduced that companies must take action on the matter so that there is a DPD within their payroll, which constitutes a figure with important functions and responsibilities, which does not necessarily have to be a lawyer, but a person who have knowledge of information security to handle or know issues such as: legal and regulatory aspects in data security, risk management under ISO 31000, ISO 25000, information security under ISO 27001, IT service management, ISO 20000, CISO (Chief Information Security Officer) security audit.

The recently approved "Data Protection" Law of Ecuador includes this role for public companies since a progressive plan is required so that the role of "Data Protection Delegate" is also extended to all private...
companies, where said plan involves educational entities so that professionals specialized in both systems law and digital law to fill this position. This SOWA matrix instrument allowed to demonstrate that internal and external forces that reflect weaknesses and strengths; Threats and opportunities are related and articulated based on generating an opinion matrix to establish the appropriate strategies in solving the problem of data security in Ecuador and the need to have the figure of a Data Protection Delegate.

6. References

[1] Unión Europea, Reglamento General de Protección de Datos, 2018.

[2] C. Jay Hoofnagle, Bart van der Sloot y F. Zuiderven Borgesius, «The European Union general data protection regulation: what it is and what it means,» Information & Communications Technology Law, vol. 28, nº 1, pp. 65-98, 10 2 2019.

[3] Q. Chen and R. A. Bridges, "Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware," in Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware, Cancún, 2018.

[4] Plan V, «La peor filtración de datos en la historia del Ecuador al descubierto,» 16 9 2019. [En línea]. Available: https://www.planv.com.ec/historias/sociedad/la-peor-filtracion-datos-la-historia-del-ecuador-al-descubierto.

[5] Asamblea de la República del Ecuador, Constitución de la República del Ecuador, Quito, 2018.

[6] Asamblea Nacional del Ecuador, «asambleanacional.gob.ec,» 10 5 2021. [En línea]. Available: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/63464-proyecto-de-ley-organica-de-proteccion.

[7] A. Ross and T. Moore, "The Economics of Information Security," Science, vol. 314, pp. 610-613, 27 10 2006.

[8] BBC and E. Paté-Cornell, "On “Black Swans” and “Perfect Storms”: Risk Analysis and Management When Statistics Are Not Enough," International Journal, vol. 32, no. 11, pp. 1823-1833, 02 03 2012.

[9] Nurmi, J., & Niemelä, M. S., "PESTEL Analysis of Hacktivism Campaign Motivations," Lecture Notes in Computer Science, p. 323–335, 2018.

[10] L. L. Lazzari and V. Maesschalek, "CONTROL DE GESTIÓN: UNA POSIBLE APLICACIÓN," no. 5, pp. 71-90, 2002.

[11] J. R. Llerena Zegarra, "UNSA," 2016. [Online]. Available: http://repositorio.unsa.edu.pe/handle/UNSA/3362.

[12] M. Albers, Reloading Data Protection - Chapter 11: Realizing the Complexity of Data Protection, Springer, 2014, pp. 213-235.

[13] AEPD, «Agencia Española de Protección de Datos,» 2018. [En línea]. Available: https://www.aepd.es/. [Último acceso: 10 2018].

[14] F. D’ALESSIO, El proceso Estratégico. Un enfoque de Gerencia, 2da. ed., México DF:: Pearson Educación, 2013, p. 714.

[15] J. L. Ramirez Rojas, "DSpace," 2017. [Online]. Available: http://148.202.167.116:8080/xmlui/handle/123456789/1214. [Accessed 31 01 2019].
[16] A. Vasquez, "IMAP - Albia Capital," 2017. [Online]. Available: https://albiacapital.com/ciberseguridadvenderempresa/#. [Accessed 31 01 2019].

[17] L. Wik, S. Horkay, K. Van Kamp, P. Rivièrè and International M&A Partners, "Imap," 03 2018. [Online]. Available: https://www.imap.com/media/uploads/publications/cybersecurity_report_18april18_fina_few_amends_pdf. [Accessed 4 02 2019].

[18] Risk Based Security, Data Breach QuickViewReport First Quarter 2019-Data Breach Trends, 2019.

[19] CISCO, "Reporte anual de Ciberseguridad 2018," CISCO, 2018.

[20] CISCO, "SERIE DE CIBERSEGURIDAD DE CISCO 2019 Reporte de Privacidad de Datos," CISCO, 2019.

[21] H. Martin, "Avast," 20 12 2018. [Online]. Available: https://blog.avast.com/biggest-data-breaches.

[22] C. Photopoulus, Managing Catastrophic Loss of Service Data, 04: Elsevier, 2008, p. 400.

[23] T. C. Mayorga-Jácome, M. García-Jiménez, J. F. Duret-Guiérrrez, J. Carrión-Jumbo and P. V. Yarad Jeada, "Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos," Dominios de la Ciencia, vol. 5, no. 1, pp. 518-537, 1 2019.

[24] K.-L. Wang, «A Study on Building of Sports Data Sharing,» Journal of Advances in Information Technology, vol. 6, pp. 54-58, 5 2015.

[25] A. M. Sreekanth Rallapalli y R. R. Gondkar, «Improving Healthcare-Big Data Analytics for Electronic Health Records on Cloud,» Journal of Advances in Information Technology, vol. 7, nº 1, pp. 65-68, 2016.

[26] S. Tangirala, «Efficient Big Data Analytics and Management through the Usage of Cloud Architecture,» Journal of Advances in Information Technology, vol. 7, nº 7, 11 2016.