International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 17 (2017) pp. 6741-6750

Experience in Applying the Analysis and Risk Management Methodology called MAGERIT to Identify Threats and Vulnerabilities in an Agro-industrial Company

[1,2]Ricardo Guagalango Vega, [2]Rubén Arroyo and [2,3,*]Sang Guun Yoo

[1]Centro de Posgrados, Universidad de las Fuerzas Armadas ESPE, Av. General Rumiñahui s/n, Sangolquí, Ecuador.

[2]Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas ESPE, Av. General Rumiñahui s/n, Sangolquí, Ecuador.

[3]Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, Ladrón de Guevara, E11-253, Quito, Ecuador.

[*]ORCID ID: 0000-0003-1376-3843, Scopus Author ID: 36187649600

Abstract

The present work focuses on sharing our experience in applying the methodology MAGERIT to identify threats and vulnerabilities that could be materialized in risks and affect company's financial statements. The present work was executed in a real company of the Agro-industrial field. The research results indicate that the application of ISO/IEC 270000 standard with the help of MARGERIT and PILAR is an excellent combination for identifying the risks and proposing the controls to mitigate them, to improve the Information Security Management of an organization.

Keywords: MAGERIT, PILAR, risk analysis, vulnerabilities

INTRODUCTION

Security have become an important area since organizations are managing more valuable assets, such as databases and information systems, each day. This is the reason why many researchers have focused in providing different security solutions in different areas [1-3].

In this aspect, organizations that develop their security strategies for the digital business must consider that Information Security not only applies to technology, but it also involves the processes and people who are part of the company. It is imperative to mention that many companies are reactive towards information security and implement computer solutions that generate significant expenses which are not reflected in return on investment. To justify the security investments, it must be done by measuring the Return on Security Investment (ROSI) [4] i.e. analyzing the economic benefits that the investments could deliver to the organization. This is possible by executing the risk analysis that allow to understand the vulnerabilities and threats that the company owns and the security measures that will allow to prevent or avoid the detected risks [5].

In this paper, we share our experience in executing the risk analysis of an Agro-industrial company in Ecuador that handles critical and sensitive information. Along this paper, we will demonstrate how a systematic methodology can help the detection of threats and vulnerabilities to then establish prevention and correction measures.

The present paper is organized as follows. First, section 2 explains briefly the standards, methodology and tool used for this research. Then, section 3 details the security risk analysis executed in the mentioned company. Later, section 4 discusses and evaluates the results obtained in section 3. Finally, section 5 concludes this work.

BACKGROUND

For the management of Information Security, there are a worldwide standard called ISO/IEC 27000 [6-8] which aims to establish the minimum requirements to comply with an Information Security Management System (ISMS). The standard ISO/IEC 27000 was developed by a Joint Technical Committee of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) and it comprised of a series of standards.

For the development of this paper, we have used the principal and most important standard denominated ISO/IEC 27001 [9] which contains the requirements of the Information Security Management System (ISMS) and it is distributed in 14 domains [10] which are: (1) Information security policies, (2) Organization of information security, (3) Human resource security, (4) Asset management, (5) Access control, (6) Cryptography [11], (9) Physical and environmental security, (10) Operations security, (11) Communications security, (12) Systems acquisition, development and maintenance, (13) Supplier relationships, (14) Information security incident management [12], (15) Information security aspects of business continuity management, and (16) Compliance with internal requirements, such as policies, and with external requirements, such as laws.

Additionally, we also have applied the ISO/IEC 27002 which delivers the good information security practices [13].

Additional to ISO/IEC 27000, the Methodology of Analysis and Management of Risks of Information Systems (MAGERIT) v.3 [14] was also used to make a better risk analysis. MAGERIT is a methodology created by the Spanish governmental organization called Consejo Superior de Administración Electrónica to meet their corporate strategic objectives. This methodology, that allows a systematic execution of risk analysis, contemplates the following phases:

1. Identify the assets with the greatest relevance and value to the organization, and what detriment or cost it would cause their degradation.
2. Establish threats to which the identified assets are exposed.
3. Determine safeguards or controls that can mitigate the identified threats and their effectiveness.
4. Estimate the impact i.e. the damage to the asset due to the materialization of a threat
5. Assess the risk, using the impact formula weighted with the occurrence rate of the threat.
6. Establish safeguards or controls to mitigate, accept, eliminate or transfer risks that have a high impact.

When applying the methodology MAGERIT, a tool called PILAR (developed by the Centro Criptológico Nacional) can be used. Such tool has a standard library capable to generate ratings based on the international ISO/IEC 27002 standard. The ISO/IEC 27002 standard includes the code of good practices for information security management.

IMPROVEMENT OF INFORMATION SECURITY PROCESSES

First, to improve the security processes of the Company, it was necessary to know the current situation of the Department of Technology and Information. For this purpose, interviews and surveys were carried out to the personnel. The controls indicated in ISO/IEC 27001 were taken and questions were transformed for each domain with true/false answers to evidence the percentage of compliance. Fig. 1 below shows the obtained results. The results indicates that the Department of Technology and Information is compliant with 62% of most of the ISO/IEC 27001 domains. It also indicates that the 38% of necessary controls have not been applied to strengthen the Information Security of the Company.

Subsequently, it was necessary to verify the genuineness of the obtained results, so it was imperative to apply the MAGERIT methodology to carry out the risk analysis based on the following process:

i) **Identification of information assets.** At this stage, technological assets relevant to the Company were identified to analyze their risks. After identifying the main assets of the technological area, these were entered to the PILAR tool to know their main vulnerabilities and the threats that could exploit those vulnerabilities.

ii) **Valuation of assets.** PILAR tool allows to measure the value of each asset based on the following dimensions:

   a. Availability (represented by [D]): It ensures authorized collaborators to access to the information and assets when they require them.
   b. Integrity (represented by [I]): It protects data and information from unauthorized modification or deletion.
   c. Confidentiality (represented by [C]): It ensures information/assets access only to authorized users [15].
   d. Authenticity (represented by [A]): It identifies users who generated the information and block the possibility of impersonation.
   e. Traceability (represented by [T]): It make possible to track who did what and when [17].

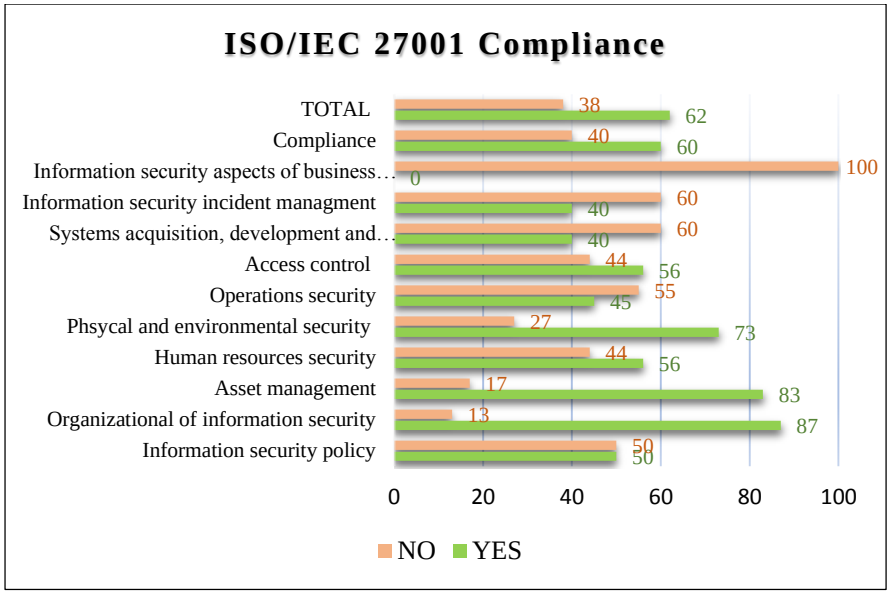


Figure 1: Percentage of Compliance of ISO/IEC 27001's Domains

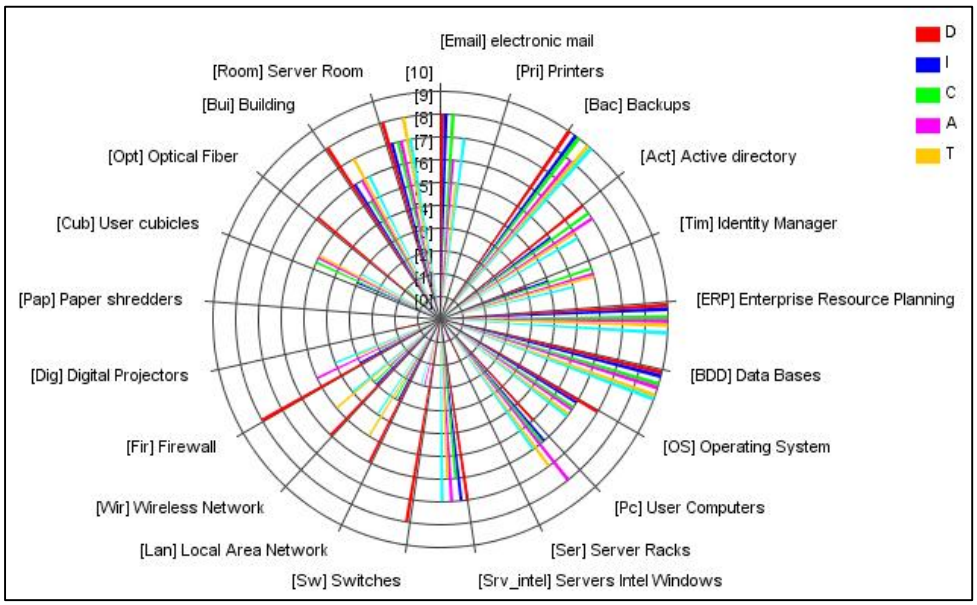


Figure 2: Identification and valuation of assets

Fig. 2 shows the identified assets generated by PILAR with their valuation. Such figure indicates that the most valuable assets for the organization are: Enterprise Resource Planning (ERP) and databases.

iii) **Threats identification.** This stage identifies the threats that may have an impact on information assets. PILAR tool includes a library with the most common threats, such as:

- Nature threats, such as earthquakes, floods, fire, among others.
- Environmental threats (industrial origin), such as pollution, electrical failures, breakdowns, etc.
- Defects of applications/equipments (due to defects in its design or its implementation).
- Accidents caused by people. People with access to the information system can cause unintentional problems, either by mistake or by omission.

- Problems caused deliberately by people. People with access to the information system can cause problems intentionally.

Tables 1 and 2 show the main threats to the most critical information assets of the company, organized by the dimensions indicated before in this sections. In the tables, the frequency of such threats can also be observed (1=once a year, 10=monthly, 100=daily, 0.2=every several years; this probability of occurrence was defined by the guidance of the technology department's staff of the company).

Table 1: Percentage of impact caused by threats related to the ERP resource

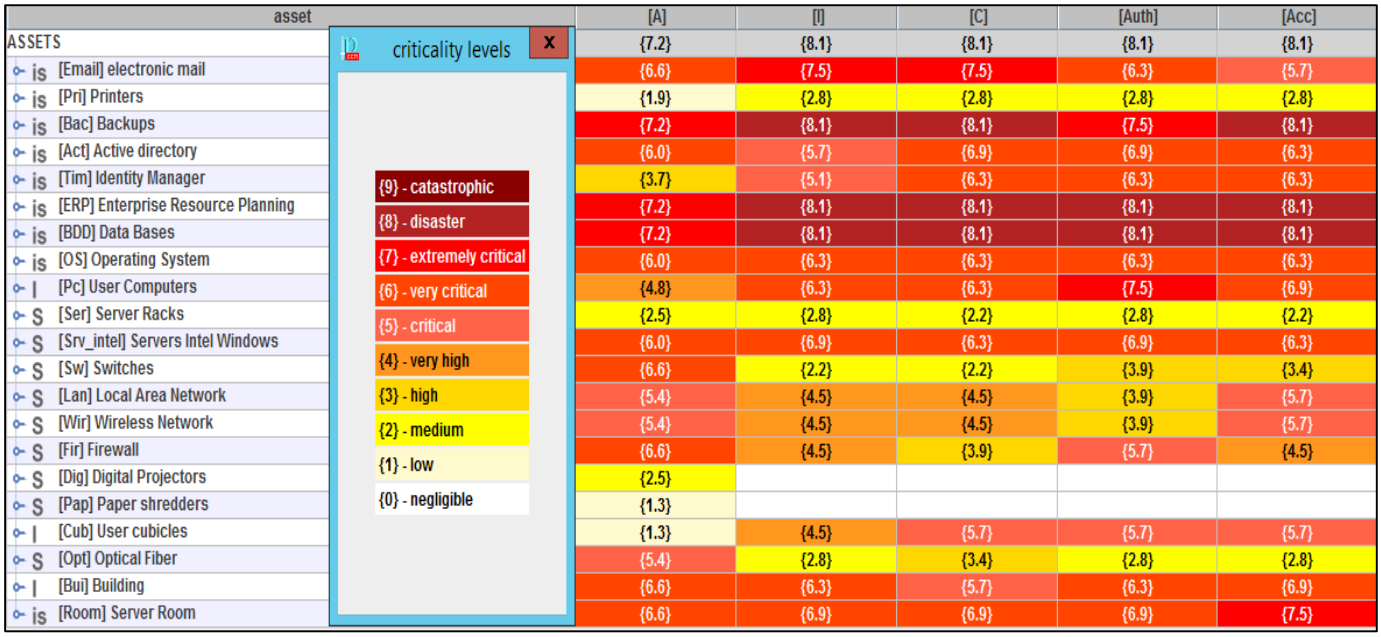
Threat	**Frequency**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[I.5] Fault of physical or logical origin	1	-	-	-	-	-
[I.9] Interruption of other essential services or supplies	1	20%	-	-	-	-
[E.1] User Errors	1	-	10%	10%	-	10%
[E.2] System Administrator or Security Errors	1	30%	20%	20%	-	-
[E.3] Monitoring errors (log)	1	-	1%	-	-	60%
[E.8] Diffusion of harmful software	1	80%	10%	10%	-	20%
[E.15] Alteration of information	1	10%	10%	100%	10%	20%
[E.18] Destruction of information	1	-	30%	-	-	10%
[E.19] Information leaks	1	-	-	100%	-	-
[E.20] Vulnerabilities of programs (software)	1	-	20%	20%	-	-
[E.21] Errors of maintenance / Software update	10	10%	1%	-	-	-
[E.24] Depletion of the system due to resource depletion	10	10%	-	-	-	-
[A.3] Manipulation of activity logs	100	-	50%	-	-	30%
[A.5] Impersonation of identity	0,2	-	100%	100%	100%	10%
[A.6] Abuse of access privileges	1	-	10%	10%	100%	-
[A.7] Unplanned use	1	-	10%	10%	-	-
[A.11] Unauthorized access	1	-	10%	50%	100%	-
[A.13] Repudiation (denial of actions)	1	-	-	-	60%	100%
[A.15] Modification of information	1	40%	90%	-	-	-
[A.18] Destruction of information	1	20%	100%	30%	-	10%
[A.19] Disclosure of information	1	-	-	90%	-	-
[A.22] Manipulation of programs	1	10%	100%	100%	-	20%
[A.24] Denial of Service	1	100%	-	-	-	-

Table 2: Percentage of impact caused by threats related to the Database resource

Threat	**Frequency**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[I.5] Fault of physical or logical origin	1	-	-	-	-	-
[I.9] Interruption of other essential services or supplies	1	20%	-	-	-	-
[E.1] User Errors	1	-	40%	40%	-	10%
[E.2] System Administrator or Security Errors	1	30%	60%	90%	-	-
[E.3] Monitoring errors (log)	1	-	100%	-	-	60%
[E.8] Diffusion of harmful software	1	80%	40%	10%	-	20%
[E.15] Alteration of information	1	10%	100%	100%	10%	20%
[E.18] Destruction of information	1	-	90%	-	-	20%
[E.19] Information leaks	1	-	-	100%	-	-
[E.20] Vulnerabilities of programs (software)	1	-	10%	20%	-	-
[E.21] Errors of maintenance / Software update	10	10%	1%	-	-	-
[E.24] Depletion of the system due to resource depletion	10	10%	-	-	-	-
[A.3] Manipulation of activity logs	100	-	100%	-	-	30%
[A.5] Impersonation of identity	0,2	-	100%	100%	100%	10%
[A.6] Abuse of access privileges	1	-	10%	10%	100%	-
[A.7] Unplanned use	1	-	10%	10%	-	-
[A.11] Unauthorized access	1	-	10%	50%	100%	-
[A.13] Repudiation (denial of actions)	1	-	-	-	60%	100%
[A.15] Modification of information	1	40%	100%	-	-	-
[A.18] Destruction of information	1	20%	100%	30%	-	10%
[A.19] Disclosure of information	1	-	-	90%	-	-
[A.22] Manipulation of programs	1	10%	100%	100%	-	20%
[A.24] Denial of Service	1	100%	-	-	-	-

iv) **Impact and risk.** With the information of threats, it is possible to establish the impact, which can be defined as the measure of the damage on the asset derived from the materialization of a threat [17]. Knowing the value of the assets (in their different dimensions) and the degradation caused by the threats, it is possible to identify the impact that these would cause on the system. The impact is calculated for each information asset according to the related threats and dimensions.

Figure 3, shows the list of the assets with the highest valuation with highest criticality levels. The results obtained using the PILAR tool indicate the level of compliance of the domains of ISO/IEC 27002 standard. It is important to consider that the safeguards or controls to be applied are associated with the controls of ISO/IEC standard. The fulfillment and implementation of the recommendations will strengthen the security of the Company.



asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS	{7.2}	{8.1}	{8.1}	{8.1}	{8.1}
[Email] electronic mail	{6.6}	{7.5}	{7.5}	{6.3}	{5.7}
[Pri] Printers	{1.9}	{2.8}	{2.8}	{2.8}	{2.8}
[Bac] Backups	{7.2}	{8.1}	{8.1}	{7.5}	{8.1}
[Act] Active directory	{6.0}	{5.7}	{6.9}	{6.9}	{6.3}
[Tim] Identity Manager	{3.7}	{5.1}	{6.3}	{6.3}	{6.3}
[ERP] Enterprise Resource Planning	{7.2}	{8.1}	{8.1}	{8.1}	{8.1}
[BDD] Data Bases	{7.2}	{8.1}	{8.1}	{8.1}	{8.1}
[OS] Operating System	{6.0}	{6.3}	{6.3}	{6.3}	{6.3}
[Pc] User Computers	{4.8}	{6.3}	{6.3}	{7.5}	{6.9}
[Ser] Server Racks	{2.5}	{2.8}	{2.2}	{2.8}	{2.2}
[Srv_intel] Servers Intel Windows	{6.0}	{6.9}	{6.3}	{6.9}	{6.3}
[Sw] Switches	{6.6}	{2.2}	{2.2}	{3.9}	{3.4}
[Lan] Local Area Network	{5.4}	{4.5}	{4.5}	{3.9}	{5.7}
[Wir] Wireless Network	{5.4}	{4.5}	{4.5}	{3.9}	{5.7}
[Fir] Firewall	{6.6}	{4.5}	{3.9}	{5.7}	{4.5}
[Dig] Digital Projectors	{2.5}				
[Pap] Paper shredders	{1.3}				
[Cub] User cubicles	{1.3}	{4.5}	{5.7}	{5.7}	{5.7}
[Opt] Optical Fiber	{5.4}	{2.8}	{3.4}	{2.8}	{2.8}
[Bui] Building	{6.6}	{6.3}	{5.7}	{6.3}	{6.9}
[Room] Server Room	{6.6}	{6.9}	{6.9}	{6.9}	{7.5}

Figure 3: Accumulative risk assessment

recom...		control	current	target	PILAR
		[27002:2013] Code of practice for information security controls	32%	49%	57%
2		[5] INFORMATION SECURITY POLICIES	10%	50%	50%
7		[6] ORGANIZATION OF INFORMATION SECURITY	50%	50%	35%
		[7] HUMAN RESOURCE SECURITY	n.a.	n.a.	
6		[8] ASSET MANAGEMENT	38%	50%	48%
7		[9] ACCESS CONTROL	41%	38%	52%
9		[10] CRYPTOGRAPHY	10%	50%	65%
6		[11] PHYSICAL AND ENVIRONMENTAL SECURITY	39%	50%	72%
9		[12] OPERATIONS SECURITY	20%	50%	73%
9		[13] COMMUNICATIONS SECURITY	49%	50%	81%
7		[14] SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE	13%	50%	44%
6		[15] SUPPLIER RELATIONSHIPS	30%	50%	81%
5		[16] INFORMATION SECURITY INCIDENT MANAGEMENT	50%	50%	68%
6		[17] INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	17%	50%	74%
5		[18] COMPLIANCE	46%	50%	61%

Figure 4: Domain Compliance Percentages of ISO/IEC 27002 Standard

Fig. 4 shows (in percentages) the current situation and the expected goals to be achieved by applying the safeguards indicated by the software PILAR.

v) **Application of safeguards.** In this phase, it is necessary to consider the following aspects for the identification and valuation of safeguards. (1) The type of assets to be protected, each type is protected in a different way. (2) Threats to which the asset requires protection. (3) If there are alternative or additional safeguards. (4) Focus on the most important risks.
It should be noted that there are different types of protection provided by safeguards [17]:

- [PR] Preventive: When the chances of an incident occurring are reduced, e.g. pre-production tests.
- [CR] Corrective: Executed after damage. The damage is repaired and reduced, e.g. incident management.
- [DC] Detective: The event is reported when an attack occurs, e.g. anti-virus.

The safeguards will be applied to those domains with a lower percentage of compliance of ISO/IEC standard since they have greater risks. These domains are as follows.

DOMAIN: INFORMATION SECURITY POLICY	
Current: 10%	Goal: 50%
ISO/IEC 27001 Controls	
• "Management must define, approve, publish and communicate to the workers and external parties involved, a series of policies for information security". • "Information security policies should be reviewed at planned intervals or if significant changes occur to ensure their continued suitability, adequacy and effectiveness".	
Safeguards to be applied	
The information security policy should have the following activities: • [G.3.3.1] Be approved by the Information Security Committee • [G.3.3.2] Specify what is proper use and misuse. • [G.3.3.3] Specify the responsibility of the people regarding their compliance and violation. • [G.3.3.4] All the personnel that are part of the organization must have access to the documents. • [G.3.3.6] Be regularly reviewed.	
Date of implementation: Immediate	

DOMAIN: SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE	
Current: 13%	Goal: 50%
ISO/IEC 27001 Controls	
• It should include the security of the information related to the requirements in the requirements of new information systems or in the improvement of existing information systems. • Information that passes through public networks should be protected from fraudulent activities, contractual disputes, and disclosure and unauthorized modifications. • You must protect the information that comes from the transaction services application, to avoid incomplete transmissions, diversions, duplicate or unauthorized reproduction of messages.	
Safeguards to be applied	
• [NEW.S.4.1] There must access control requirements must be considered. • [NEW.S.4.2] There must consider identification and authentication requirements. • [14.2.2] There must be procedures to control changes in systems. • [14.2.3] There must be technical revisions of the applications after making changes to the operating system. • [14.2.4] There must be restrictions on changes to software packages. • [NEW.SW.6.6.2] There must be a separation of functions between the personnel that develops and the personnel in charge of production. • [14.2.9] There must be user acceptance tests for systems that go into production by external suppliers [18].	
Date of implementation: September 2017	

DOMAIN: INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGMENT	
Current: 17%	Goal: 50%
ISO/IEC 27001 Controls	
• The organization must determine its requirements for information security and for the continuity of information security management in adverse situations. For instance: During a crisis or disaster. • The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity of information security during an adverse situation. • The organization must verify the controls of the continuity of the information security established and implemented, at regular intervals with the purpose of assuring its validity and effectiveness during adverse situations.	
Safeguards to be applied	
• [BC.BIA] There must do a *Business Impact Analysis (BIA)* [19]. • [BC.BIA.2] The assets involved in critical processes must be identified. • [BC.BIA.3] Recovery targets should be established for each critical process *Recovery Time Objective (RTO*) [20] • [BC.BIA.4] Recovery targets should be established for each critical information *Recovery Point Objective (RPO)* [20].	

• [BC.DRP] There must generate a *Disaster Recovery Plan (DRP)* [21]. • [BC.1.2.3] Tests should be performed and the incidents detected should be analyzed as if they had occurred on the base system. • [17.2.1] There must be redundancy to ensure the availability of information processing resources [22].
Date of implementation: December 2018

vi) **Impact and residual risk analysis.** This is the last stage and it allows the analysis of results after implementation of the safeguards. It allows to measure the modification of impact and the risk from a potential value to a residual value. Fig. 5 and 6 show the impact and residual risk results after applying safeguards recommendations.

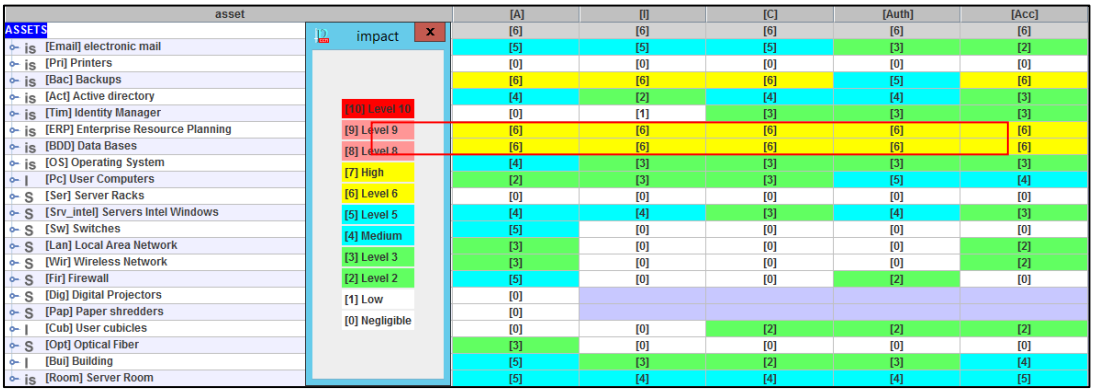


Figure 5: Residual impact analysis

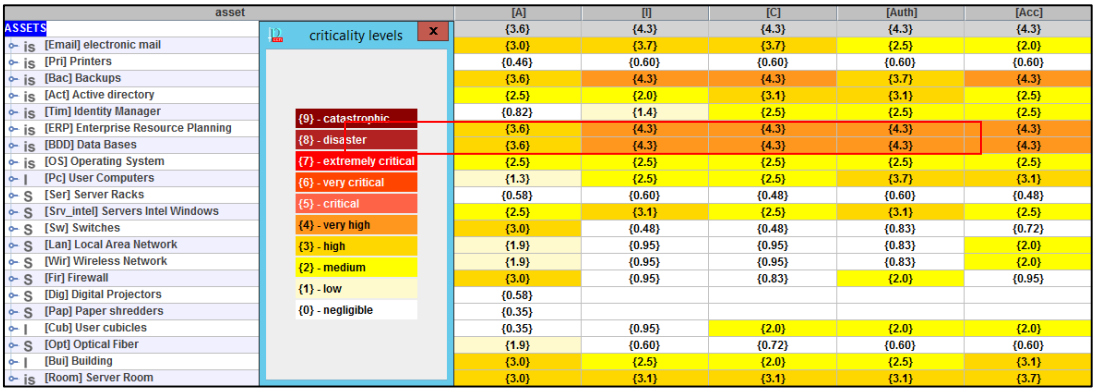


Figure 6: Residual risk analysis

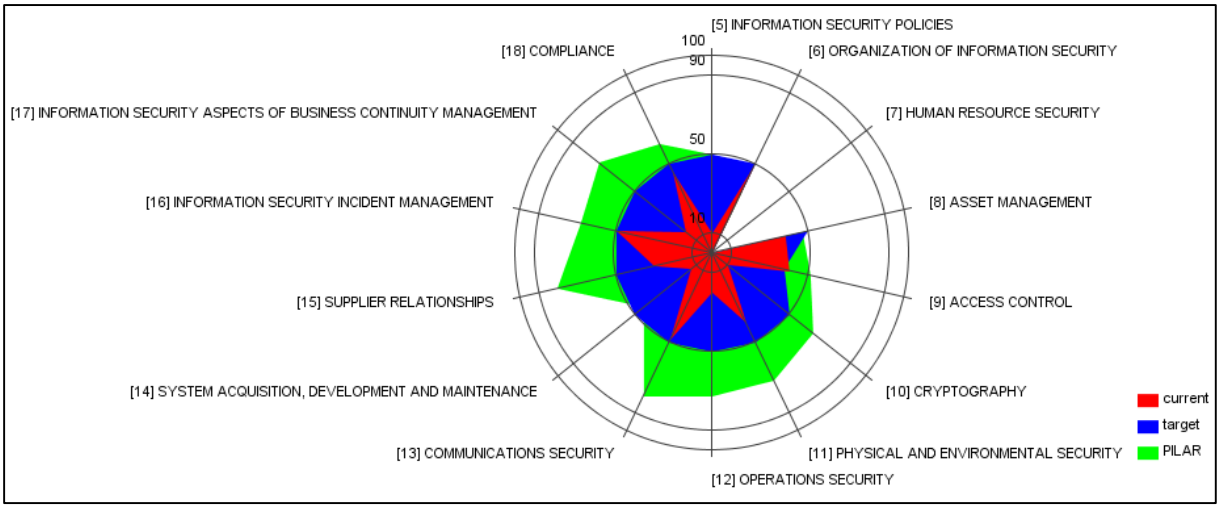


Figure 7: Evolution phases of ISO/IEC 27002 Standard

After applying the mentioned safeguards or controls, the level of evolution of ISO/IEC 27002 standard improved significantly. Fig. 7 shows the maturity levels from the current situation to the situation recommended by PILAR.

EVALUATION OF RESULTS AND DISCUSSION

Based on the obtained results, it was possible to observe that the domains with the highest percentage of compliance were Organizational of information security with 87% and Asset management with 83% (in the current situation phase). On the other hand, the domains with the lowest degree of compliance was Information security aspects of business continuity management with 100% of non-compliance, which means that no type of control had been applied. It is important to consider that these results were obtained through interviews and questionnaires with the staff of Technology and Information.

In order to have a greater degree of certainty of results, it was necessary to carry out the risk analysis. The first phase consisted on identifying and valuing the main assets; in this phase the Enterprise Resource Planning (ERP) and Databases were detected as more valuable ones. Threats that primarily degraded assets were impersonation, spreading harmful software, and manipulation of programs.

To improve the security of these assets, it was necessary to start the improvement process of the information security management. This was able by identifying the domains of ISO/IEC 27001 standard with the highest percentage of non-compliance extrapolated with the assets with the highest threats and establishing the necessary safeguards. The domains detected with lower percentage level was the Information Security Policy with 10%. When considering safeguards, improvement of security level from 10% to 50% was set as the expected goal of this domain. Smilar goal was established with the domain of Systems acquisition, development and maintenance from 13% to 50%. To reduce the identified risks of ERP application and Databases, the domains related to the field of information systems, operating systems, applications, infrastructure, services, databases were strengthened by ensuring the secure software development, modification in control procedures in systems, technical revisions of applications after making changes, restrictions on software packages chances, use of engineering principles in systems protection, security in environments development, functional tests during the development of systems, acceptance tests, etc. The mentioned controls allowed to reduce the possibility of occurrence of threats related to impersonation, malicious software dissemination, and program manipulation.

Similarly, the goal of percentage of compliance of the domain of Information security aspects of business continuity management was set to 50% (from 17%). This will allow the Company to be prepared for possible risks such as natural disasters and security breaches.

CONCLUSIONS

This paper has identified a methodology called MAGERIT and it was used to perform the risk analysis focused on assessing the current situation of Information Security in the Department of Technology and Information of a real company applying the ISO/IEC 27000 standard. This work also complemented such analysis by using the PILAR software. This process allowed to report safeguards and controls to mitigate threats and to know the maturity level of each domain of ISO/IEC 27001 standard of the analyzed Agro-industrial Company. The risk analysis report allowed investors and executives to be informed of required investments related to the Information Security with the best Return on Security Investment.

REFERENCES

[1] Yoo, S., Park, K., and Kim, J., 2012, “Confidential information protection system for mobile devices,” Security and Communication Networks. Vol 5, issue 12, pp. 1452-1461, Doi: 10.1002/sec.516

[2] Park, K., Yoo, S., and Kim, J. 2011, “Security Requirements Prioritization Based on Threat,” Modeling and Valuation Graph, Proceedings of International Conference on Hybrid Information Technology, pp. 142-152.

[3] Yoo, S., Lee, H., and Kim, J., 2013, “A Performance and Usability Aware Secure Two-Factor User Authentication Scheme for Wireless Sensor Networks,” International Journal of Distributed Sensor Networks 2013(2), DOI: 10.1155/2013/543950

[4] Sonnenreich, W., 2006, “Return on security investment (ROSI)-a practical quantitative model,” New York, pp. 45-56.

[5] Peltier, T. R., 2005, “Information Security Risks Analysis,” Second ed., T. &. F. Group, Auerbach Publications, p. 163.

[6] Peltier, T. R., 2016, "Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security," Auerbach Publications, pp. 175-187.

[7] Calder, A., 2009, "Information Security based on ISO 27001 / ISO 27002 - A Management Guide," Second ed., Van Haren Publishing, p. 85.

[8] [Disterer, G., 2013, "ISO/IEC 27000, 27001 and 27002 for Information," Scientific Research, pp. 2-5.

[9] Susanto, H., 2012, "Information Security Challenge and Breaches: Novelty Approach on International Journal of Engineering and Technology, " Vol. 2, p. 9.

[10] Suduc, A. M., 2010, "Audit for Information Systems Security," 14(1), p. 43.

[11] Ahituv, N., 1987, "Processing encrypted data. Communications of the ACM," Reserach Contribution, 30(9), p. 4.

[12] Baskerville, R., 2014, "Incident-centered information security: Managing a strategic balance between prevention and response," Information & Management, 51(1), pp. 138-151.

[13] Sojčík, P., 2012, "Tools for information security managment," p.48.

[14] Verdún, J., 2006, "The risks analysis like a practice of secure. A revision of models and methodologies," 5th IFIP International Conference on Network Control & Engineering for QoS, Security and Mobility, Madrid.

[15] Zevin, S., 2009, "Standards for security categorization of federal information and information systems," National Institute of Standards and Technology, p. 9.

[16] Withman, M., 2003, "Enemy of the gate: threats of information security," Kennesaw, Georgia, 46(8).

[17] Bass, T., 2001, "Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations," Milcom 2001, Vienna, pp. 1-10.

[18] Sualim, S. A., 2017, "Comparative Evaluation of Automated User Acceptance Testing Tool for Web Based Application," International Journal of Software Engineering and Technology, 2(2), p. 6.

[19] Radeschütz, S., 2010, "BIAEditor: matching process and operational data for a business impact analysis," In Proceedings of the 13th International Conference on Extending Database Technology, pp. 1-4.

[20] Keeton, K., 2004, "Designing for disasters," In Fast, Vol. 4, pp. 59-62.

[21] Hawkins, S., 2000, "Disaster recovery planning: a strategy for data," Information Management & Computer Security, Vol. 8, pp. 222-229.

[22] Huffman, D., 1952, "A Method for the Construction of Minimum-Redundancy Codes," Procedings of the J.R.E., 40(9), pp. 1098-1101.