Acceptance Level Factors for Security Policies Compliance on Employees

Paola Casandra Martínez Bravo
Universidad Autónoma de Guadalajara
pbravo@edu.uag.mx

PhD Juan Mejía Trejo
Universidad de Guadalajara
juanmejiatrejo@hotmail.com

Abstract - This paper discusses the possible reasons for the employees to accept or not the security policies implemented in their organizations. This is something that every organization must be aware of because a great percentage of the attacks are originated from the inside by an employee who –consciously or unconsciously- is not following the procedures and standards that the policies described. This information will be useful to the organizations to help them to protect one of their main assets, data.

Keywords—Security policies, employees, acceptance level

I. INTRODUCTION

"Security policies are IT responsibility". "They only exist to make work even harder". "There is no reason to follow them, everything will be the same".

The previous statements could be common to the IT's area when it attempts to introduce a new security policy inside the organization. Change resistance, ignorance or indifference could cause a rejection toward it, without giving it the chance to prove its value.

For any organization, the decision to implement a security policy and obtain the compliance of its employees with it could have a huge impact. But, why is so important to be aware of all of this?

CSI/FBI point out that 72% of organizations reported a security breach in 12 months and a 52% a non-authorized use of the computer assets. [25].

Previous studies about information security, suggests that 91% of the employees frequently fail with actual compliance with the security policies of the organization [20]. It is estimated that American organizations lost $63 billion every year due to employees' abuse on the Internet. [3]. Most of 71% of the employees would be willing to divulge their computer password for nothing more than a chocolate bar [23].

All of these data offer a brief perspective about how serious for an organization could be not to have security policies and the compliance of its employees towards them.

For that reason, this study pretends to identify the main factors involved in the success or failure in the employees' compliance with a security policy.

The next section presents a brief history about the threats and computing security evolution to highlight the security policies importance; in addition some back ground about prior researches that described employees' behavior towards security policies.

The rest of the paper is presented as follows: the research model and data collection instrument and finally the conclusions about the research.

II. BACK GROUND

Information security history starts with computer security, which arose during World War II when the firsts mainframes, developed to break communication codes where used [25].

At the end of 60's the Defense Advanced Research Projects Agency developed a computer experimental network to exchange military information, it was called ARPANET (Advanced Research Project Agency NETwork). However, the first security problems appeared immediately. The remote user sites do not have enough controls and safeguards to protect the information from non-authorized users [25].

On 1970, the *Security Controls for Computational Systems* report was published, which recommendations guide a great number of programs dedicated to protect classified information and to establish standards for its protection [19].

At the same decade, the DOD (Department of Defense) sponsored additional researches focusing on security policies model development [19].

In 1983, the standard TCSEC (Department of Defense Trusted Computer System Evaluation Criteria) was published, commonly known as Orange Book, which describes evaluation criteria that is used to establish security levels in a particular system. From it, European standards like ITSEC and international standards like ISO/IEC 17799 were developed [19].

In the last years technology development has increased considerably; devices allow connecting to network at any given time and place, entertainment and storage media with huge capacity. Nevertheless, they came with big information threats that have grown up and evolved at the same speed.

The emerge of threats which compromise the confidentiality, integrity and availability of information has provoked the development of a wide range of technology, processes, devices and security standards, from hardware –like firewalls and IDS- and software –as antivirus and antispam- to international standards as ISO17799 or BS13335, which purpose is to guarantee information security.

Among these tools we find security policies. In their simplest form can be defined as high level documents which purpose is to be a guide inside the organizations to establish metrics that must be applied to protect the information.

But, even with these tools, organizations could be still victims of their own weaknesses and suffer the consequences of internal and external attacks.

The solution to this problem is subject of discussion between security professionals. A possible solution is not to launch tools against a security threat problem, but to improve security processes and people around the technologies that the organization already has. [25].

Almost all the attacks that the organizations suffer come from the inside. Therefore, if the employees receive the proper training on how to protect the information based on the security policies established, the number of problems related to security will be diminished.
Is important for the employees to be aware of the wrong doings, and its consequences; the more information they have the more comprehension about their purpose could guide to a better results.

III. SECURITY POLICIES AND HUMAN BEHAVIOUR

Security is based on people. "If you think that technology can solve security problems then you do not understand problems or technology". [24].

A security policy is a high level document that expresses the way in which an organization has to protect the data. They should be interpreted and supported by standards, procedures and guides [24]. The policies have to follow the SMARTE rule, which means, Specific, Measurable, Achievable, Realistic, Traceable and Enforceable [14].
According to norm PN-I-13335-1:9999: *The security policy of an institution in the field of IT systems: principles, directives and procedures, which determine how the resources – including vital information – are being managed, protected and distributed within the institution and its IT systems [12]*.
Kevin Beaver (2010) points out that the first step to implement a security policy is to know all the organization risks, and who will be affected once it is implemented. Besides, emphasizes the importance of not just consider simple things –like passwords or Internet use- while defining the contents of a policy, it is necessary to consider all the scenarios that can be helpful to improve the information protection.
The main purpose of security programs, policies and standards is to protect the significant assets inside an organization, specially: data.
It is important not to confuse security policies with plans or procedures; security policies only specify "how to do things", the other ones, point out how they should be implemented, achieved and managed.
Organizations have very clear the value to invest on market research to identify customer needs, motivation and lifestyles; but they fail to spend a similar time and money on their employees. But, is it not through employees that all organizational results are achieved? [26].
Privacy and awareness training about information security is a challenge in every organization [24]. It is necessary to consider all the risks that involve the fact of not having a security culture on every employee.
Everyone is responsible for security policies, management, manufacturing, staff, IT and Human Resources, etc. Everyone has to know and apply them; otherwise they will end up as documents which anybody knows. Security policies development process, distribution and employees' awareness about them have to be high level priorities [7].
It is important for each security policy to be easy to comprehend; to be clear and simple from the very beginning and also define its scope and purpose [7]. Otherwise, it would be as bad as not to have any security policy at all. It has to be considered that these documents will be read by people who are not security experts, that is why the excessive use of technical words that could make them difficult to understand have to be avoided. Besides, it is necessary to go through them frequently to ensure their effectiveness, especially because new systems and technologies are developed at high speed and the user needs change [5].
Also, the security policies must not evolve into disorganized and complex documents which employees are afraid to read because they are impossible to understand and apply [6]. These documents must be aligned to the business' objectives and goals, otherwise they could cause harm instead of benefits.
Hagen (2009) points out the presence of some barriers that employees have to overcome before they can behave as expected about the security policies. A barrier is the lack of knowledge and the incapacity to recognize the possible security breaches.
Among the elements that are provided to the employees to help them to overcome these obstacles, are training and some other tools. However, sometimes these are not enough, because is necessary to know which factors are intervening in the lack of compromise on people.
Nowadays education about information security is focused on technical aspects, security mechanisms and attacks; but computer security education could benefit from including more subjects and ideas from economics, ethics, organization theory and psychology [8].
Blanke (2008) studied the factors that intervene on computational abuse intentions from employees, which mainly are: attitude, security policies awareness and self-efficacy; being the first and third the ones that proved to have a real bond.
Intentions have been recognized as the main element of Social Psychology [3]. In addition, there are more interesting for the psychologists than any other social motives because of their main role on the direction and channeling of social conduct [4].
The attitude that an employee has towards security can cause the compliance or not with it; studies made in Norway proved that many times people behave according to imitation of their coworkers of immediate boss, which suggests the importance of social influence in the security policies compliance [8].
In addition, behavior literature has recognized that observing people that is important to the employee tends to affect employee's behavior [22].
The awareness purpose of security policies is that every employee needs to know what can be or cannot be done [3] and the consequences for every action [22]. However, programs designed to motivate this have been inefficient in practice, because employees understand the policies as difficult to learn, inappropriate and freedom restrictive [3].
Self-efficacy is defined as a judgment of one's capability to organize and execute course of actions required to follow certain behavior [3]. It refers not to the abilities of someone but to "the judgments about what can or cannot be done with them". Some studies [3] provide evidence about the fact that self-efficacy affects the reactions from an individual to technology.

Threats and vulnerabilities' evaluations and the severity perception of them, have an effect on the employee's intentions to follow the security policies [22].

According to the Protection Motivation Theory, an element known as Threat Appraisal, divided in Perceived vulnerability and Perceived severity, has influences on the employee's intention to fulfill security policies. The former one refers to the evaluation that the employee makes about the probability that a negative event will take place in the organization if no one takes measures to counter it. The latter one encompasses both the physical and psychological harm a potential threat might cause for the employee and the organization [22]. It is necessary that the employees understand the harm that a security breach might cause, because if they are not capable to perceive this risk they would not be able to follow a security policy as it is needed.

Information quality has been seen as decisive to identify factors that could affect the success of information systems [18]. As mentioned before, it is of vital importance that security policies are made in a clear form that allows everyone to understand them. The way in which information is presented to the employees can influence on their final decision to accept or not what is established.

Two different approaches have been adopted by some organizations to encourage the security policies compliance on their employees, each of them being the opposite from the other: penalties and rewards.

There are different opinions about these concepts, and their utility on the employee's behavior. While some authors mention the scanty efficiency of them, other said that if they are used in a proper way, it is possible to obtain the expected results. In summary: Not many organizations have been able to use monetary incentives as a reliable method to increase quality and quantity in manufacturing [13].

According to Siponen et al. (2010) the use of rewards -tangibles and intangibles- has an insignificant effect on security policies compliance. In addition, it is difficult to generalize the rewards on a group of employees, because something can work for someone but not for the rest [22].

On the other side, penalties; that can be a warning, a temporal or definitive suspension –depending on the gravity of the action-; have proven to be more effective to achieve the security policies compliance [22]. When this method is used, it is really important that the penalties are applied immediately after the action is made.

Any other technique of approach adopted to motivate the employees to follow the security policies, has to take into account certain conditions before results can be evaluated, like the fact that the employees will need some time to adjust to the policies, to have access to them and all the support to understand and apply them [18].

All the studies that have been discussed in this paper have been made on countries like: USA, England, Norway and Finland; however, none of them take in consideration Latin-American countries; this research is planned for Mexican organizations, thus, some of the variables can have a different impact on this society even though the result is different from the rest of the countries.

On the basis of all above information, the following hypotheses are proposed:

H1: The intention to follow a security policy has influence in the compliance.

H2: Awards have a positive effect on security policies compliance.

H3: Penalties to employees that do not follow security policies have a positive effect on security policies compliance.

IV. STUDY CASE

Even with all the technological tools that the organizations have to guarantee their security information, the reality is that almost all of them are still suffering the consequences of security breaches.

There are many authors that coincide in the fact that the security must be based on, first of all, people [7][24][25]; however, literature also points out that this is the element that receives less attention [7][26]. Statistics results show that more than 90% of the attacks and security problems, came from the inside of the organization [3][5][20].

If an organization realizes how important is the participation of the employees on security and decides to adopt some metrics to deal with this situation, which aspects have to be considered?

For all these reasons, this research has the purpose of identifying all the elements that have some influence on the employees' acceptance and security policies compliance.

V. CONSIDERATIONS

This study will allow the management levels of organizations to know the factors in which they have to invest time and other resources to achieve a high level of commitment from the employees towards security policies.

The first step is to determine if the organizations that provide IT services have a high level of acceptance and fulfillment of security policies on their employees. If they are involved with technology it is expected to have satisfactory results and even higher that the ones of those organizations that do not have a lot of information about security.

If an organization has the commitment of the employees with the security policies, they could have a significant decrease in the security breaches produced within them. Besides, data will be protected against different scenarios related with human beings or with nature.

The research is limited to employees of Mexican organizations, and to be more specific those located at Jalisco state which main activity is related with IT.

Due to the difference among cultures of every country, and even the different thoughts between states, the results obtained here cannot be generalized to a bigger population.

Another aspect to consider is the fact that the information type that would be required from the employees could be considered as sensitive and they could feel threaten or intimidated at the moment of response. For this reason, all the surveys will be applied guarantying anonymous answers.

However, the risk of fear affecting the answers has to be considered when the surveys are created and applied and when the results are analyzed.

VI. METHODOLOGY

To prove the proposed hypotheses, a methodological matrix was designed based on the independent variables: Intention, Rewards and Penalties, with their proper dimensions and indicators. After that, this was the base to create a measurement instrument prototype that will be used to determine it these variables have an influence on the compliance level for security policies.

This is a co-relational study because its purpose is to prove if a relation exists between the independent and dependent variables.

The measurement instrument consists of questions to measure the agreement or disagreement, conformity or nonconformity levels and similar subjects for every indicator; it is based on the Likert scale and statistical methods will be used to verify if the hypotheses are valid or not.

The sample consists of some organizations related with IT on Jalisco. Table 1 shows the economic units that the estate has according to the data obtained by INEGI on the economic census of 2004 [28].

TABLE I. INEGI – ECONOMIC CENSUS 2004

Sector	**Economic Units**
Computer, communication and measurement equipment manufacture, and electronic accessories.	71
ISP, network services and data processing.	32
Software	123
Other telecommunications	158
Other information services	14
	Total: 398

Source: INEGI 2004

Based on the previous information, and having a total of 398 organizations divided in 5 sectors whose main activities are realized on the IT area the sample size to perform this research can be determined using the formula proposed by [17]. (1)

$$n = \frac{z^2pqN}{Ne^2 + z^2pq} \quad (1)$$

Being *n* the sample size, *z* whished confidence level (95%), *p* success probability (0.5), *q* failure probability (0.5), *e* estimation error (0.05) and *N* the universe (398)

According to this formula and considering the mentioned values, the optimum sample size is 195 organizations.

The final objective will be to identify if a relation exists between the independent and dependent variables.

TABLE II. METHODOLOGICAL MATRIX FOR INDEPENDENT VARIABLE: INTENTION

Conceptual Definition: Purpose to do or achieve an objective [27].			
Operational Definition: It indicates the purpose of doing something and they are good predictors of the real behavior, which could be affected by attitudes, self-efficacy and quality information [21].			
Dimension	**Indicator**	**Q**	**Author**
Attitude	Social Influence	1, 2	Herath & Raghav (2009); Malcolmson (2009); Siponen, Pahnila & Mahmood (2006); Siponen (et al. 2009); Pahnila (et al. 2007).
	Threats Evaluation	3, 4	Malcolmson (2009); Pahnila (et al. 2007); Siponen (et al. 2006); Siponen (et al. 2010).
Self-efficacy	Visibility	5, 6	Siponen (et al. 2009); Siponen (et al. 2006); Siponen (et al. 2010); Wilmot (1987).
	Conscious	7, 8	Blanke (2008); Dowell (2004); Januszkiewicz (2007); Hu, Hart & Cooke (2006); Siponen (et al. 2006); Smith (2006)
Information Quality	Perceived Importance	9, 10	Pahnila (et al. 2007)
	Perceived Utility	11 - 13	Pahnila (et al. 2007)

TABLE III. METHODOLOGICAL MATRIX FOR INDEPENDENT VARIABLE: REWARDS

Conceptual Definition: Gratification received by a service of favor; is a reinforcement of any type that increases the possibility of that response [16].			
Operational Definition: Rewards can be used to increase interest and motivation [22].			
Dimension	**Indicator**	**Q**	**Author**
Interest	Interest Level	14	Pahnila (et al. 2007); Siponen (et al. 2010)
Motivation	Motivation Level	15	Pahnila (et al. 2007); Siponen (et al. 2010)

TABLE IV. METHODOLOGICAL MATRIX FOR INDEPENDENT VALUE: PENALTIES

Conceptual Definition: A penalty is any consequence that diminishes the likelihood for any particular response, it adds something unpleasant to the environment, so the behavior is weaken [16].			
Operational Definition: Penalties are originated by the Deterrence General Theory, which suggests that certain, severity and velocity affect people decisions [18].			
Dimension	**Indicator**	**Q**	**Author**
Certain	Certain Level	16, 18	D'Arcy y Hovav (2004), quoted by Herath (et al. 2009); Pahnila (et al. 2007)
Severity	Severity Level	17, 18	D'Arcy y Hovav (2004), quoted by Herath (et al. 2009); Pahnila (et al. 2007)
Velocity	Velocity Level	19	Pahnila (et al. 2007)

Based on these matrix Fig. 1, 2 and 3 are proposed, they summarize the relation of the variables with their dimensions and indicators and the authors that support it.

Finally, Fig. 4 presents a detail conceptual model ex ante, which shows the independent variables and their effect on the dependent variable.

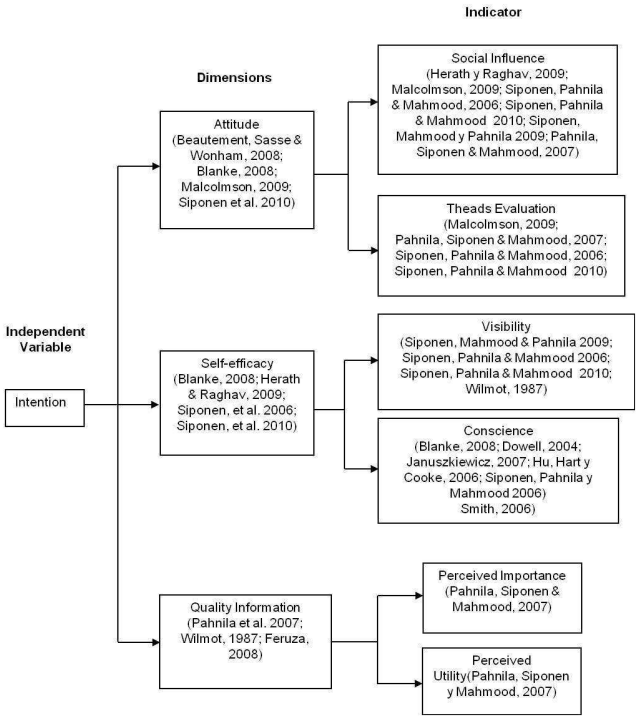

Figure 1. Independent Variable Intention.

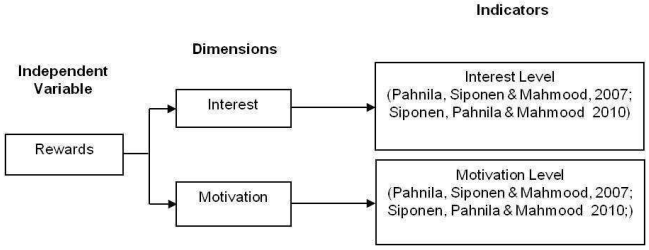

Figure 2. Independent Variable Rewards.

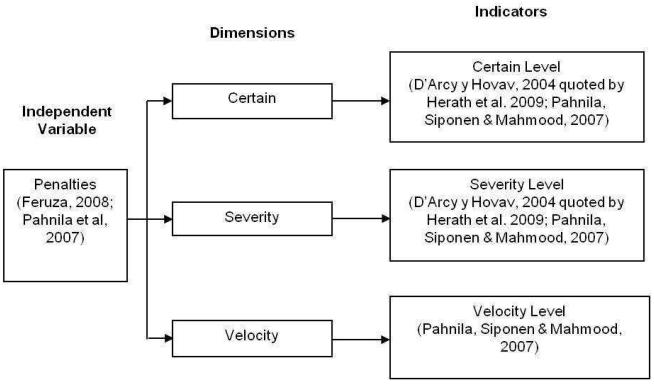

Figure 3. Independent Variable Penalties.

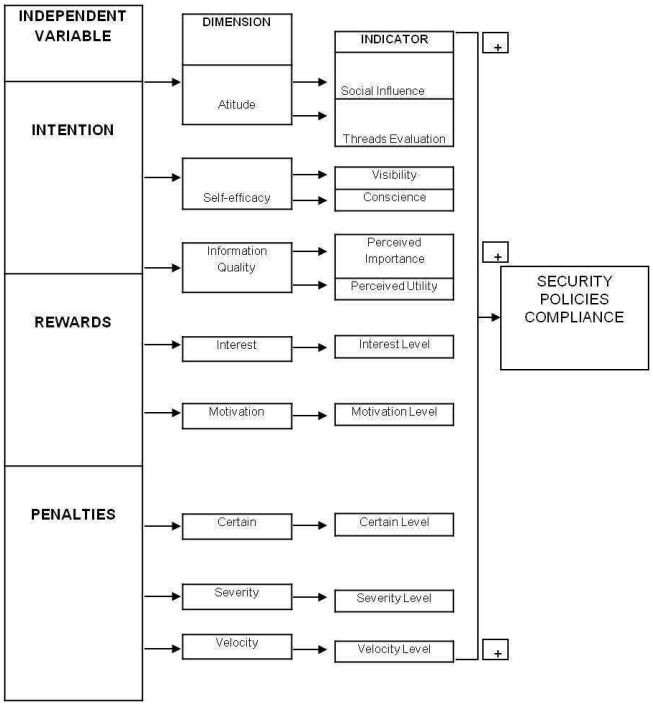

Figure 4. Conceptual Detail Model ex ante.

VII. MEASUREMENT INSTRUMENT

The results for every survey can have values according to the Tables 5, 6 and 7.

TABLE V. VALUE RANGE

Minimum Value	Maximum Value
1	19

TABLE VI. VALUE RANGE FOR EVERY VALUE

Variable	Questions	Minimum	Maximum
Intention	1-13	13	65
Reward	14-15	2	10
Penalty	16-19	4	20
Security policies compliance	1-19	19	95

TABLE VII. TOTAL

Minimum Value	Maximum Value
19	95

TABLE VIII. MEASUREMENT INSTRUMENT

1. I usually follow the recommendations that my boss or coworkers give about security policies.
2. I always try to help my coworkers to follow the security policies.
3. I think that any security breach inside my organization will have an effect on me.
4. If I detect a security breach, I report it and behave according to what is established.
5. Security policies are properly distributed inside the organization.
6. The security policies are located in an accessible place that allows me to consult them whenever I need.
7. I know the existence and content of the security policies.
8. I am conscious about the consequences that can be generated against me or the organization if I do not follow the security policies.
9. The information given to me allows me to comprehend the importance of the security policies.
10. The information use related to security increments the value of our duties.
11. Information provided about security policies is easy to understand.
12. The existent information is useful to know how to react in case of any security breach.
13. The information is applicable to our tasks.
14. For me, is important to receive incentives or praises from my superiors.
15. The organization usually provides rewards for security policies' compliance.
16. If I do not follow the security policies, I will get a penalty.
17. Penalties given for any fault committed against information security are severe.
18. I follow with all the security measures indicated in the security policies to avoid any penalty.
19. Penalties are applied every time that a security policy is broken, immediately after the incident.

VIII. CONCLUSIONS

Security is a topic that any organization no matter its scope, market or size can let at a side. Security guards, keys, passwords, encryption, access control, ACLs, firewalls, antivirus and many other tools fight every second against a very long list of threats: virus, worms, hackers, crackers, not authorized access, DoS, manipulation, theft and information lost.

The first thought for many people is that there are specific groups whose only purpose is to break organizations security and cause information damage. However, even though it is a real problem, is not as bad as the attacks that are originated within the organization.

Unfortunately, attacks caused by employees, in a conscious or unconscious way, generate more problems and security breaches than any external threat.

Information security becomes a vital aspect and an effective way to protect it and involve everyone in this process is the use of security policies.

This research pretends to point out the elements that have the most significant influence in the employee's acceptance process towards a security policy. In base of prior research it could be inferred that intentions are the main factor that affects this process.

For punishments and awards, is more complex to predict their correlation and the degree in which they could affect the final employee's behavior. The reason for this is that there are too many factors that could influence people to one side or the other. These kinds of variables have to be carefully defined before any measurement instrument can be applied. To establish if the awards would be tangibles or intangibles and the period of time in which they would be given. For the penalties the employees have the right to know everything about them, like duration, severity and any other characteristic that could influence the reaction towards them.

Once all the factors are identified, the organization has to acquire a compromise at every level to follow the security policies and to invest all the resources that are needed to promote the employees' compliance with them according with the expected results.

IX. REFERENCES

1. Beautement, A.; Sasse, M.; Wonham, M. The Compliance Budget: Managing Security Behaviour in Organisation. 2008.
2. Beaver, K. Security Policy Oversights and Mistakes We Keep Making. 2010.
3. Blanke, S. A study of the Contributions of Attitude, Computer Security Policy Awareness and Computer Self-Efficacy to the Employee's Computer Abuse Intention in Business Environments. 2008.
4. Clay, H. Introducción a la Psicología Social. 3rd Ed. México: Trillas. 1995.

5. Corbitt, T. Protect your computer system with a security policy. 2002.
6. Dowell, K. Info Security Policy Tips. 2004.
7. Feruza, S. Advanced Security Policy Implementation for Information Systems. 2008.
8. Hagen J. Human Relationships. A Never-Ending Security Education Challenge? 2009.
9. Herath, T.; Raghav H. Protection motivation and deterrence: a framework for security policy compliance in organizations. 2009.
10. Hernández, R.; Fernández, C.; Baptista, P. Metodología de la Investigación. 4th Ed. México: Mc Graw Hill. 2008.
11. Hu, Q.; Hart, P.; Cooke, D. The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective. 2006.
12. Januszkiewicz, P. Designing a Security Policy According to BS 7799 Using the OCTAVE Methodology. 2007.
13. Katz, D. *Psicología Social de las Organizaciones.* 2nd Ed. México: Trillas. 1989.
14. Madigan, E.; Petrulich, C.; Motuk, K. *The Cost of Non-Compliance – When Polices Fail.* 2004.
15. Malcolmson, J. *What is Security Culture? Does it differ in content from general Organisational Culture?* 2009.
16. Morris, C.; Maisto, A. *Introducción a la Psicología*. 12th Ed. México: Pearson/Prentice Hall, p. 154-155, 2005.
17. Münch, L.; Ángeles, E. *Métodos y Técnicas de Investigación*. Ed. Trillas. 1995.
18. Pahnila, S.; Siponen, M.; Mahmood, A. *Employee's Behavior towards IS Security Policy Compliance.* 2007.
19. Russell, D.; Gangemi, G. *Computer Security Basics.* USA: Reilly. 1991.
20. Siponen, M.; Mahmood, A.; Pahnila, S. *Are employees putting your company at risk by not following information security policies?* 2009.
21. Siponen, M.; Pahnila, S.; Mahmood, A. *Factors Influencing Protection Motivation and IS Security Policy Compliance.* 2006.
22. Siponen, M.; Pahnila, S.; Mahmood, A. *Compliance with Information Security Policies: An Empirical Investigation.* 2010.
23. Smith, M. *The Importance of Employee Awareness to Information Security*. 2006.
24. Tipton, H.; Krause, M. *Information Security Management Handbook.* 6th. Ed. Nueva York: Auerbach Publications, p. 378, 465, 499, 645, 2006.
25. Whitman, M.; Mattord, H. *Principles of Information Security.* 3th. Ed. Boston: Course Technology, p 389, 2007.
26. Wilmot, D. *Management Undervalues Employee Potential.* Communication world. 1987.
27. *Academia de la Real Lengua Española*, 23th Ed. , July 27, 2010 from http://buscon.rae.es
28. *Sistema de Consulta de los Censos Económicos 2004.* August 4th, 2010.