RIICO 2015

"La Competitividad frente a la Incertidumbre Global"

RIICO 2015

IX Congreso de la Red Internacional de Investigadores en Competitividad

11-13 Noviembre 2015
Guadalajara-Jalisco

LA COMPETITIVIDAD FRENTE A LA INCERTIDUMBRE GLOBAL

MEMORIAS

Coordinadores:
Sánchez Gutiérrez José
Mayorga Salamanca Paola Irene
González Uribe Elsa Georgina

Distribución RIICO 2015- Guadalajara, Jalisco 11-13 de noviembre 2015
Red Internacional de Investigadores en Competitividad

ISBN: 978-607-96203-0-4

THE SECURITY INFORMATION POLICIES AND THE EMPLOYEES IN THE SOFTWARE SECTOR: AN EMPIRICAL STUDY IN MEXICO

Mejía Trejo Juan [1]
*Sánchez Gutiérrez José**
*Vázquez Ávila Guillermo***

ABSTRACT

This study is aimed to discover the reasons for the employees to accept or not the Security Information Policies implemented in their organisations (**SIPC**), in México. **Five Factors** are considered: Attitude (**ATT**); Self Efficacy (**SEF**); Information Perceptions (**IFP**); Rewards (**REW**) and Penalties (**PNY**) with **21 Variables** as indicators. A questionnaire was designed and applied to **195** employees involved in the **SME** Software Sector in Guadalajara (**SSG**) México that conform the value chain, including: designers, manufacturers and suppliers; the confidence was measured with **Cronbach's Alpha** (**.87**) and it was applied Structural Equations Modelling (**SEM**) to discover the **3 SIPC** underlying variables in the mode The organisations must be aware about these results, because a great percentage of the attacks are originated from inside by an or few employees who consciously (or not) are not following the procedures and standards that the policies described.

Keywords—Security Information Policies, Employees, Software Sector in México.

[1] Universidad De Guadalajara- Centro Universitario De Ciencias Económico Administrativas

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 organisation. Change resistance, ignorance or indifference could cause a rejection toward it, without giving it the chance to prove its value. For any organisation, 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 organisations reported a security breach in 12 months and a 52% a non-authorized use of the computer assets. [Whitman & Mattord, 2007]. Previous studies about information security, suggests that 91% of the employees frequently fail with actual compliance with the security policies of the organisation [Siponen et al.,2009]. It is estimated that American organisations lost $63 billion every year due to employees' abuse on the Internet. [Blanke, 2008]. Most of 71% of the employees would be willing to divulge their computer password for nothing more than a chocolate bar [Smith, 2006]. All of these data offer a brief perspective about how serious for an organisation 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 rest of the paper is presented as follows: the contextual reference of **SSG**, the problem, research questions, the theoretical framework, methodology, the questionnaire, the validity and reliability of the model results, discussion, conclusions and finally, the **SEM** resulting model.

CONTEXTUAL REFERENCE

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 [Whitman & Mattord, 2007]. 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 [Lehtinen & Gangemi, 2006]. At the same decade, the DOD (Department of Defense) sponsored additional researches focusing on security policies model development [Lehtinen & Gangemi, 2006]. 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 [Lehtinen & Gangemi, 2006]. 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 [Hu & Cooke, 2006], 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 organisations to establish metrics that must be applied to protect the information. But, even with these tools, organisations 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 organisation already has. [Whitman & Mattord, 2007]. Almost all the attacks that the organisations 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.

PROBLEM, RESEARCH QUESTIONS, RATIONALE FOR THE STUDY

So, our problem is described in a General Question (**GQ**), as: ¿Which are the latent factors in **ATT, SEF, IFP, REW** & **PNY** on **SIPC** relationship? The rationale of the study is due the interest of **SSG** companies to identify such latent factors in the employees. The Specific Questions (**SQ**), were: **SQ1**.-What are the Variables as indicators of the general conceptual model?; **SQ2**.-What are the relationships of these variables?; **SQ3**.-What are the most relevant variables of the model?. The Hypotheses (**H**) to be demonstrated are: **H1:** *A high level of **ATT** generates a high level of **SIPC** in the **SSG**;* **H2:** *A high level of **SEF** generates a high level of **SIPC** in the **SSG**;* **H3:** *A high level of **IFP** generates a high level of **SIPC** in the **SSG**;* **H4:** *A high level of **REW** generates a high level of **SIPC** in the **SSG**;* **H5:** *A high level of **PNY** generates a high level of **SIPC** in the **SSG**.*

THEORETICAL FRAMEWORK

Security is based on people. "If you think that technology can solve security problems then you do not understand problems or technology" [Tripton & Krause, 2006]. A security policy is a high level document that expresses the way in which an organisation has to protect the data. They should be interpreted and supported by standards, procedures and guides [Tripton & Krause, 2006]. The policies have to follow the SMARTE rule, which means, Specific, Measurable, Achievable, Realistic, Traceable and Enforceable [Feruza, 2008][Madigan et al., 2004]. 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 [Januszkiewicz, 2007]. Some works points out that the first step to implement a security policy is to know all the organisation risks, and who will be affected once it is implemented [Beaver, 2010]. 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 organisation, 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. Organisations 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 organisational results are achieved? [Wilmot, 1987]. Privacy and awareness training about information security is a challenge in every organisation [Tripton & Krause, 2006]. 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 [Feruza, 2008]. 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 [Feruza, 2008]. 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 [Corbitt, 2002][Siponen et al.,2009][Siponen et al.,2006]. 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 [Martínez-Bravo & Mejía-Trejo, 2011]. These documents must be aligned to the business' objectives and goals, otherwise they could cause harm instead of benefits. Some studies [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, organisation theory and psychology [Clay, 1995][Hagen, 2009][Katz, 1999]. Some studies treat the factors that intervene on computational abuse intentions from employees [Blanke, 2008], 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 [Blanke, 2008][Clay, 1995][Katz, 1999]. 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 [Beautement et al., 2008][Clay, 1995][Katz, 1999]. 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 [Hagen, 2009]. In addition, behaviour literature has recognized that observing people that is important to the employee tends to affect employee's behaviour [Siponen et al.,2010]. The awareness purpose of security policies is that every employee needs to know what can be or cannot be done [Blanke,2008] and the consequences for every action [Siponen et al.,2010]. However, programs designed to motivate this have been inefficient in practice, because employees understand the policies as difficult to learn, inappropriate and freedom restrictive [Blanke,2008]. Self-efficacy is defined as a judgment of one's capability to organize and execute course of actions required to follow certain behaviour [Blanke,2008]. It refers not to the abilities of someone but to "the judgments about what can or cannot be done with them". Some studies [Blanke,2008] 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 [Siponen et al.,2010]. 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 organisation 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 organisation [Siponen et al.,2010]. 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 [Pahnila, et al., 2007]. 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 organisations 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 behaviour. 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 organisations have been able to use monetary incentives as a reliable method to increase quality and quantity in manufacturing [Katz, 1999]. The use of rewards - tangibles and intangibles- has an insignificant effect on security policies compliance [Siponen et al.,2009][Siponen et al.,2006]. 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 [Siponen et al.,2010]. 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 [Siponen et al.,2010]. 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 at LatinAmerican countries; this research is planned for Mexican organisations, 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. Even with all the technological tools that the organisations 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 [Feruza, 2008][Tripton & Krause, 2006][Whitman & Mattord, 2007]; however, literature also points out that this is the element that receives less attention [Feruza, 2008][Wilmot, 1987]. Statistics results show that more than 90% of the attacks and security problems, came from the inside of the organisation [Blanke,2008][Corbitt, 2002][Siponen et al.,2009]. If an organisation 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.

METHODOLOGY

This study will allow the management levels of organisations 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 organisations that provide IT services have a high level of acceptance and fulfillment of security policies on their employees. The research is limited to employees of Mexican organisations, 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. 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 by Structural Equations Modeling (**SEM)** that will be used to determine the underlying variables that influence on the compliance level for security policies. The measurement instrument consists of questions to measure the agreement or disagreement, conformity or nonconformity levels and similar subjects for every indicator based on the Likert. The sample consists of some organisations related with IT on Jalisco. **See Figure 1** that shows the economic units of Jalisco State has according to the data obtained by INEGI on the economic census of 2014 [INEGI, 2014].

Figure 1. **INEGI – Economic Census 2014**

Sector Economic Units	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, 2014

Figure 2, summarizes the most relevant aspects of the research carried out.

Figure 2.- Technical Research Data

Features	Survey
Universe	398 employees belonging to the **SSG**
Scope	Metropolitan City of Guadalajara, México
Sample Unit	**SME´s** from **SSG** over 10 employees
Collection Method of Data	e-Mail
Scale	Likert 5
Date of Fieldwork	June-November 2014
Total e-Mail completely answered	**195**

Source: Own

Based on the previous information [Hernández et al., 2008] [Münch & Angeles, 2005], and having a total of **195** organisations divided in **5 sectors** whose main activities are realized on **SSG,** we proceed to apply a questionnaire via census, as is shown in **Figure 3.**

Figure 3.- **Questionnaire (To Discover The Relationships On SIPC=F6)**

Factor	Variable	AUTHOR(S)
Attitude (ATT=**F1**)	**V1.-** I usually follow the suggestions that my boss or coworkers give about security policies. **V2.-** I always try to help my coworkers to follow the security policies.	[Beaver, 2010]; [Clay, 1995]; [Herath & Raghay, 2009];[Katz, 1999] ;[Malcolmson, 2009]; [Morris & Maisto, 2005]; 18]; [Siponen et al.,2009]; [Siponen et al.,2006]
	V3.- I think that any security breach inside my organisation will have an effect on me. **V4.-** If I detect a security breach, I report it and behave according to what is established.	[Blanke,2008]; [Hagen, 2009]; [Malcolmson, 2009]; [Pahnila, et al., 2007]; [Siponen et al.,2006]; [Siponen et al.,2010]; [Tripton & Krause, 2006]
	V5.- The information is the most important company's asset of and I care of that.	[Corbitt, 2002]; [Siponen et al.,2006]; [Siponen et al.,2010]; [Whitman & Mattord, 2007]
Self-Efficacy (SEF=**F2**)	**V6.-** Security policies are properly distributed inside the organisation. **V7.-** The security policies are located in an accessible place that allows me to consult them whenever I need	[Corbitt, 2002]; [Siponen et al.,2009]; [Siponen et al.,2006]; [Siponen et al.,2010]; [Smith, 2006]; [Wilmot, 1987]
	V8.- I am conscious about the consequences that can be generated against me or the organisation if I do not follow the security policies.	[Beaver, 2010]; [Blanke,2008]; [Martínez-Bravo & Mejía-Trejo, 2011]; 11]; [Januszkiewicz, 2007]; [Siponen et al.,2006]; [Smith, 2006]
	V9.- I know and apply the existence and content of the security policies	[Martínez-Bravo & Mejía-Trejo, 2011]; [Januszkiewicz, 2007];[Smith, 2006]
Information Perceptions (IFP=**F3**)	**V10.-** The information given to me allows me to comprehend the importance of the security policies.	[Beautement, et al. 2004]; [Corbitt, 2002]; [Feruza, 2008]; [Januszkiewicz, 2007] ; [Pahnila, et al., 2007]

	V11.- The information use related to security increments the value of our duties.	
	V12.- Information provided about security policies is easy to understand. **V13.- I'd use the information against the company, if I feel threatened me.**	
	V14.- The information's security represents a company's competitive advantage	[Corbitt, 2002]; [Januszkiewicz, 2007]; [Malcolmson, 2009]; [Lehtinen & Gangemi, 2006]
Rewards (REW=**F4**)	**V15-** For me, is important to receive incentives or praises from my superiors.	[Clay, 1995]; [Feruza, 2008]; [Herath & Raghay, 2009]; [Katz, 1999]; [Morris & Maisto, 2005]; [Pahnila, et al., 2007]; [Siponen et al.,2010]
	V16.- The organisation usually provides rewards for security policies compliance.	[Beaver, 2010]; [Clay, 1995]; [Feruza, 2008]; [Herath & Raghay, 2009]; [Katz, 1999]; [Malcolmson, 2009]; [Morris & Maisto, 2005]
	V17.- I'm always interested in proposing improvements and new forms of information security policies, because the rewards.	
Penalties (PNY=**F5**)	**V18.-** . If I do not follow the security policies, I will get a penalty	[Clay, 1995]; [Herath & Raghay, 2009]; [Katz, 1999]; [Madigan et al., 2004]; [Malcolmson, 2009] [Morris & Maisto, 2005]; [Pahnila, et al., 2007]
	V19.- Penalties given for any fault committed against information security are severe.	
	V20.- I follow with all the security measures indicated in the security policies to avoid any penalty.	
	V21.- Penalties are applied every time that a security policy is broken, immediately after the incident.	[Madigan et al., 2004]; [Pahnila, et al., 2007]; [Malcolmson, 2009]

Source: Own
Note: **SIPC= F6.-**Security Information Policies Compliance By Employees in Mexico.(**SIPC**)

VALIDITY AND RELIABILITY OF THE MODEL

Initial Conditions.-About the validity of the measurement scales, it was used the confirmatory factor analysis (**CFA**) by mean of the maximum likelihood method with **EQS 6.1** software [Bentler & Wu, 2012][Brown, 2006][Byrne, 2006]. Cronbach's *alpha* and composite reliability index (**CRI**) [Bagozzi & Yi, 1988], were used as a techniques to prove the reliability of the measurement scales. All scale values exceeded the recommended value of **0.7** for Cronbach's *alpha* and the (Composite Rate Index) **CRI**, which indicates that there is evidence and justifies internal reliability of the scales [Hair et al., 2010]. It represents the variance extracted from the group of the observed variables and the fundamental construct [Fornell & Larcker,1981], particularly, values above **0.6** are desirable [Bagozzi & Yi, 1988]. The settings used in this study were: the Normed Fit Index **(NFI)**, the Non-Normed Fit Index (**NNFI**), the Comparative Fit Index (**CFI**) and the Root Mean Square Error of Approximation (**RMSEA**) [Bentler & Wu, 2012]; [Byrne, 2006]; [Bentler, 1990] [Hair et al., 2010] [Chau, 1997][Heck, 1998]. Values of **NFI**, **NNFI** and **CFI** between **0.80 and 0.89** represent a reasonable fit [Hair et al., 2010] and a value equal to or greater than **0.90** represents an evidence of a good fit of the theoretical model [Byrne, 2006]. **RMSEA** Values below **0.08** are acceptable [Hair et al., 2010]

RESULTS

The **CFA** results are presented in **Figure 4** and suggests that the model provides a good fit to the data (**S-B*X*** ² = **241.4946**; df = **174**; p = **0.00054**; **NFI** = **0.907**; **NNFI** = **0.93**; **CFI** = **0.920**; **RMSEA** = **0.045**). Additionally, Cronbach's alpha and the **CRI** (>= **0.70**),recommended by [Hair et al., 2010]) and the Rate of Variance Extracted **RVE**(>=0.5) was calculated for each pair of constructs, resulting in an **RVE** more than 0.50 [Fornell & Larcker,1981]. As evidence of convergent validity, the results pointed out that all of the **CFA** items factor related are significant (p <0.001) and the magnitude of all the factorial charges is superior of **0. 60** [Bagozzi & Yi, 1988].

Figure 4. Internal Consistency and Convergent Validity of the Theoretical Model.

Factor	Variable	Factorial Charge	Robust t-Value	Loading Average	Cronbach's Alpha (>=0.7per Factor via SPSS)	CRI >=0.7	RVE >=0.5
ATT (F1)	**V3**	0.830***	1.000a	**0.820**	**0.7356**	**0.7146**	**0.6725**
	V4	0.810***	10.629				
SEF (F2)	**V7**	0.800***	1.000a	**0.815**	**0.7239**	**0.7084**	**0.6645**
	V8	0.830***	14.093				
IFP (F3)	**V13**	0.870***	1.000a	**0.885**	**0.8177**	**0.8034**	**0.7835**
	V14	0.900***	13.090				
REW (F4)	**V16**	0.790***	1.000a	**0.835**	**0.7400**	**0.7352**	**0.6993**
	V17	0.880***	14.250				
PENY (F5)	**V20**	0.840***	1.000a	**0.820**	**0.7250**	**0.7148**	**0.6728**
	V21	0.800***	12.830				

S-BX ² = 241.4946**; df** = 174**; p** = 0.00054**; NFI** = 0.907**; NNFI** = 0.93**; CFI** = 0.920**; RMSEA** = 0.045
a.- Parameters constrained to the value in the identification process.
***= p < 0.001

Source: Own

According with the evidence of the convergent validity, discriminant measure is provided in two forms as we can see in **Figure 5**. First, with a **95%** interval of reliability, none of the individual elements of the latent factors correlation matrix contains **1.0** [Anderson & Gerbing, 1988]. Second, extracted variance between the two constructs is greater than its corresponding **IVE** [Fornell & Larcker,1981]. Based on these criteria, we can conclude that the different measurements with the model show enough evidence of discriminant validity and reliability.

Figure 5. Discriminant validity of the theoretical model.

Factors	ATT (F1)	SEF (F2)	IFP (F3)	REW (F4)	PENY (F5)	CHI Square Differences Test (Values <IVE)
ATT (F1)	**0.6725**	0.437	0.181	0.141	0.121	
SEF (F2)	0.270, 0.410	**0.6645**	0.613	0.207	0.202	
IFP (F3)	0413, 0.621	0.366,0.558	**0.7835**	0.587	0.369	
REW (F4)	0.305, 0.663	0.351, 0.539	0.431, 0.639	**0.6993**	0.558	
PENY (F5)	0.300, 0.708	0.420, 0.587	0.520, 0.640	0.620,0.689	**0.6728**	
	Interval Confidence Test (<1.0)					

The diagonal represents the index of variance extracted (**RVE**), while above the diagonal part presents the variance (the correlation squared); below the diagonal, is an estimate of the correlation of factors with a confidence interval of 95%.

Source: Own

To obtain the statistical results of the research hypotheses, we applied the **SEM** as a quantitative method with the same variables to check the structure model and to obtain the results that would allow the hypotheses posed, using the software **EQS 6.1** [Bentler & Wu, 2012] [Brown, 2006][Byrne, 2006] Furthermore, the nomological validity of the theoretical model was tested using the *chi square*, through which the theoretical model was compared with the adjusted model. The results indicate that no significant differences are good theoretical model in explaining the observed relationships between latent constructs [Anderson & Gerbing, 1988][Hatcher, 1994]. Taking in account only the 10 Factors described and using again **EQS 6.1**, we obtained the **Figure 6.**

Figure 6. Results of hypothesis testing the theoretical model

Hypothesis	Structural Relation	Standardized Coefficient	t Value
H1.- A high level of **ATT** generates a high level of **SIPC** in the **SSG**.	**ATT→SIPC**	0.190***	13.552
H2.- A high level of **SEF** generates a high level of **SIPC** in the **SSG.**	**SEF→SIPC**	0.330***	15.788
H3.- A high level of **IFP** generates a high level of **SIPC** in the **SSG**.	**IFP→SIPC**	0.420***	16.876
H4.- A high level of **REW** generates a high level of **SIPC** in the **SSG**.	**REW→SIPC**	0.380***	13.258
H4.- A high level of **PENY** generates a high level of **SIPC** in the **SSG**.	**PENY-SIPC**	0.220***	10.890
S-B*X* ² (df=94)=23,6169; p=0.000 ; **NFI**=0.935 ; **NNFI**=0.917 ; **CFI**=0.9738; **RMSEA**= 0.058 ***= p < 0.001			

Source: Own

So, the results obtained after applying the **SEM** quantitative method, shows the following results:
H1 (β = 0.190, p <0. 001), the relationship between **ATT** and **SIPC** has significant positive effect.
H2 (β = 0.330, p < 0.001), the relationship between **SEF** and **SIPC** has significant positive effect.
H3 (β = 0.420, p < 0.001), the relationship between **IFP** and **SIPC** has significant positive effect.
H4 (β = 0. 380, p <0. 001), the relationship between **REW** and **SIPC** has significant positive effect.
H5 (β = 0.220, p <0. 001), the relationship between **PNY** and **SIPC** has significant positive effect.

Summarizing, we can conclude that the four variables measuring **SIPC**, are positive and significant and are very similar in terms of the value that each brings.

DISCUSSION AND CONCLUSIONS

We confirmed that the **5 Factors**, such as: **ATT, SEF, IFP, REW,PNY** are involved into the **SIPC**, with **21 Variables** as Indicators, solved the **SQ1** by mean to have proposed as theoretical framework that is showed in **Table 2**; using **SEM**, we obtained **Table 3** to solve **SQ2**, **Table 4** to solve **SQ3.** The prove of the Hypotheses by the results obtained in **Table 6,** where **H3.-** A high level of **IFP**

generates a high level of **SIPC** in the **SSG** shows the most relevant latent factor . So we solved the **GQ** at **100%.**

However, ¿how the latent variables are interacting?; to answer this, we applied the **SEM** as a quantitative technique and we can see how the underlying variables are interacting amongst them at the same time of multiple regressions are in progress. We found that only **10/21 SIPC** with **3/12 SIPC** indicators were important. In order of that, we have:

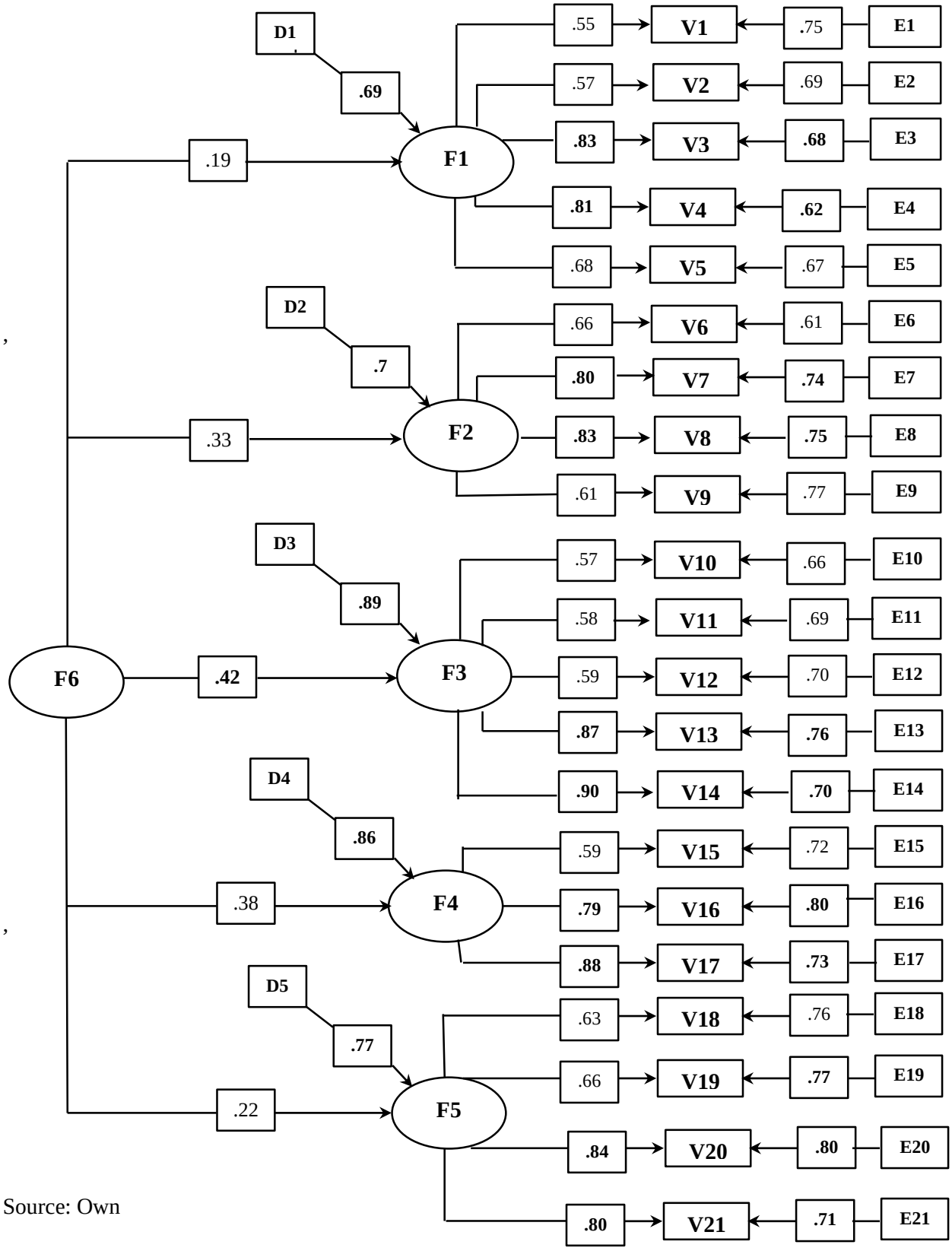
Factor: IFP (F3), V14.- *The information's security represents a company's competitive advantage*. This latent factor represents the perception of the employee with higher value in the study, because the high competition in the **SSG.** It corresponds to a employee's higher level education as a principal feature in the sector because the employee is appreciated more than an associated than an employee, by the company. [Corbitt, 2002] [Januszkiewicz, 2007] [Malcolmson, 2009] [Lehtinen & Gangemi, 2006]

Factor:REW (F4),V17.- *I'm always interested in proposing improvements and new forms of information security policies, because the rewards.*The employee is considered an important change factor in the company and all the time is required to give new ideas boosted by rewards.[Beaver, 2010] [Clay, 1995] [Feruza, 2008] [Herath & Raghay, 2009] [Katz, 1999] [Malcolmson, 2009] [Morris & Maisto, 2005].

Factor: IFP (F3), V13.- *I'd use the information against the company, if I feel threatened me.* There are a lot of cases where the emotions and other subjective reasons, impulse to the employee to do actions against the company. Some actions to prevent a potential attack, are: sudden and continuous change of passwords, assignment of special encryption, hierarchic permission use, etc.(Beautement et al., 2008; [Corbitt, 2002] [Feruza, 2008]. However, the principal actor here, is the human factor. [Januszkiewicz, 2007] [Pahnila, et al., 2007].

The Final SEM, is showed in Figure 7.

Figure 7.- Hypothesized Model of Second-Order Factor, Structure Equation Model.



Source: Own

REFERENCES

Beautement, A.; Sasse, M.; Wonham, M. (2004). The Compliance Budget: Managing Security Behaviour in Organisations. *Proceeding of the 2008 workshop on New security paradigms* p. 47-58. ACM Digital Library. Retrieved 20150304 from: http://dl.acm.org/citation.cfm?id=1595684. doi>10.1145/1595676.1595684

Beaver, K. (2010). Security Policy Oversights and Mistakes We Keep Making. Principle Logic. Information Security Policies. Retrieved 20150504 from: http://www.principlelogic.com/policies.html

Blanke, S. (2008). *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*. Doctoral Dissertation. ACM Digital Library Retrieved 20150504 from: http://dl.acm.org/citation.cfm?id=1571475

Clay, H. (1995). *Introducción a la Psicología Social.* 3rd Ed. México: Trillas.

Corbitt, T. (2002). Protect your computer system with a security policy. *Management Services;* May. 46 (5), p.20. Ebsco Host. Retrieved 20150504 from: http://connection.ebscohost.com/c/articles/12144933/protect-your-computer-system-security-policy

Martínez-Bravo, C.; Mejía-Trejo, J. (2011) Acceptance Level Factors for Security Policies Compliance on Employees. *Proceedings of 2011 IEEE International Conference on Information Theory and Information Security*. p.398-403

Feruza, S. (2008) Advanced Security Policy Implementation for Information Systems. Ubiquitous Multimedia Computing, 2008. *UMC '08. International Symposium*. p. 244-247. IEEExplore Digital Library . Retrieved 20150504 from: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4656553.DOI: 10.1109/UMC.2008.56

Hagen J.M.(2009) Human Relationships. A Never-Ending Security Education Challenge?. *IEEE Security & Privacy* 7(4):65-67. Retrieved 20150214 from: http://www.bibsonomy.org/bibtexkey/journals%2Fieeesp%2FHagen09/dblp

Herath, T.; Raghav H. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*. 18, p. 106–125. Retrieved 20150624 from: http://www.palgrave-journals.com/ejis/journal/v18/n2/abs/ejis20096a.html. DOI:10.1057/

Hernández, R.; Fernández, C.; Baptista, P. (2008) *Metodología de la Investigación.* 4th Ed. México: Mc Graw Hill.

Hu, Q.; Hart, P.; Cooke, D. (2006) The Role of External Influences on Organisational

Information Security Practices: An Institutional Perspective. *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference.* Vol.6. Retrieved 20150624 from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1579545&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F10548%2F33366%2F01579545.
DOI: 10.1109/HICSS.2006.481

Januszkiewicz, P. (2007) Designing a Security Policy According to BS 7799 Using the OCTAVE Methodology. Conference: Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference. *IEEExplore Digital Library*. . Retrieved 20150624 from: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4159867.
DOI: 10.1109/ARES.2007.69

Katz, D. (1999) Psicología Social de las Organizaciones. 2nd Ed. México: Trillas.

Madigan, E.; Petrulich, C.; Motuk, K.(2004). The Cost of NonCompliance (2004). When Polices Fail. *Proceeding SIGUCCS '04 of the 32nd annual ACM SIGUCCS conference on User services, p*. 47-51 .ACM Digital Library. Retrieved 20150624 from:
http://dl.acm.org/citation.cfm?id=1027815 .DOI: 10.1145/1027802.1027815

Malcolmson, J. (2009). What is Security Culture? Does it differ in content from general Organisational Culture*?. Proceeding Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference. IEEExplore Digital Library*. Retrieved 20150417 from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5335511&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5335511.
DOI: 10.1109/CCST.2009.5335511

Morris, C.; Maisto, A. (2005) *Introducción a la Psicología*. 12th Ed. México: Pearson/Prentice Hall, p. 154-155.

Münch, L.; Ángeles, E. (2005). *Métodos y Técnicas de Investigación.* Ed. Trillas.

Pahnila, S.; Siponen, M.; Mahmood, A. (2007) Employee's Behavior towards IS Security Policy Compliance. *Proceedings System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference*. IEEEXplore Digital Library. Retrieved 20150417 from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4076692&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4076692. DOI: 10.1109/HICSS.2007.206

Lehtinen,,R.; Gangemi, G.T. (2006). *Computer Security Basics.* USA: O'Reilly Media.

Siponen, M.; Mahmood, A.; Pahnila, S. (2009) Are employees putting your company at risk by not following information security policies?. *Communications of the ACM*, 52 (12), p.145-147. Retrieved 20150417 from:

http://cacm.acm.org/magazines/2009/12/52818-are-employees-putting-your-company-at-risk-by-not-following-information-security-policies/abstract.
DOI: 10.15/1610252.1610289
Siponen, M.; Pahnila, S.; Mahmood, A.(2006) Factors Influencing Protection Motivation and IS Security Policy Compliance. *Proceedings of Innovations in Information Technology, 2006.*IEEExplore Digital Library. Retrieved 20150623 from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4085422&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4085422.
DOI: 10.1109/INNOVATIONS.2006.301907
Siponen, M.; Pahnila, S.; Mahmood, A.(2010) Compliance with Information Security Policies: An Empirical Investigation. *Computer* 43(2). *IEEExplore Digital Library*. Retrieved 20150523 from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5410711&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5410711.
DOI: 10.1109/MC.2010.35
Smith, M. (2006) The Importance of Employee Awareness to Information Security. *Proceedings Crime and Security, 2006. The Institution of Engineering and Technology Conference.).* IEEExplore Digital Library. Retrieved 20150623 from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4123749&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4123749.
Tripton, H.; Krause, M.(2006). *Information Security Management Handbook.* 6th. Ed. Nueva York: Auerbach Publications, p. 378, 465, 499, 645,
Whitman, M.; Mattord, H.(2007). *Principles of Information Security.* 3thd. Ed. Boston: Course Technology, p. 389.
Wilmot, D. (1987). Management Undervalues Employee Potential. *Communication World.* 4(12)
INEGI (2014). Instituto Nacional de Estadística y Geografía Sistema de Consulta de los Censos Económicos 2014, México. Retrieved 20150222 from: http://www.inegi.org.mx/

About EQS 6.1

Bentler , P.M. & Wu,E.J.C. EQS 6.1(2012). *Structural Equations Program Manual*; June 20 CA: Multivariate Software Inc.
Brown, T. A. (2006*). Confirmatory Factor Analysis for Applied Research*. New York, The Guilford Press.
Byrne, B. M. (2006) *Structural Equation Modeling With EQS.Basic concepts, applications, and*

programming. London, LEA Publishers.

Bagozzi, R.P.& Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*. 16 (1): p.74-94

Hair, J. , Black, W. & Babin, B.(2010). *Multivariate Data Analysis* 7th ed. New Jersey. Prentice Hall.

Fornell, Cl. & Larcker, D. F. (1981) Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research,* 18 (2).p. 39-50.

Bentler, P.M.& Bonnet, D. (1980) Significance tests and goodness of fit in analysis of covariance structures, *Psychological Bulletin*, Sep-Dec. (88). P 588-606.

Bentler, P.M. (1990) Comparative fit indexes in structural models. *Psychological Bulletin.* 107(2). p. 238-246.

Anderson , J.,C. & Gerbing, D.,W. (1988). Structural equation modeling in practice: a review and recommended two-step approach. *Psychological Bulletin*. 1(3).p. 411-423.

Chau, P. (1997). Reexamining a model for evaluating information center success using a structural equation modeling approach. *Decision Sciences.* 28(2). P. 309-334

Heck, R.H. (1998) Factor analysis: exploratory and confirmatory approaches in Marcoulides, G.A. (Ed.). *Modern Methods for Business Research*. Mahwah, NJ Lawrence Erlbaum Associates.

Hatcher, L. (1994) *A Step by Step Approach to Using the SAS System for Factor Analysis and Structural Equation Modeling*. USA. Cary, NC: SAS Institute Inc