A Delphi approach for the establishment of the fundamental principles of an Organizational Security System in Public Administration

Victor A. Bañuls
Universidad Pablo de Olavide
vabansil@upo.es

Rafael Cantueso Burguillos
Junta de Andalucía
rafael.cantueso@juntadeandalucia.es

Fernando Tejedor Panchón
MSIG Smart Management
tejedor@msig.es

Miguel I. Ramirez de la Huerga
MSIG Smart Management
miguel.ramirez@msig.es

Murray Turoff
New Jersey Institute of Technology
Murray.turoff@gmail.com

ABSTRACT

The aim of this work is defining fundamental principles of an Internal Security System in the presence of intentional risks in Public Administration. The relevance of this object of study has increased even more with the emergence of new terrorist groups and the proliferation of organized crime, which have been categorized as a maximum threat to Security by the government. This context has led to new regulations and legislation on Security matters at the national and international level to protect assets, people and the activity of the Administration itself. Despite the large number of regulations and relevance of this topic, there is not any study which defines in a comprehensive manner the requirements that a security system must have in the presence of intentional risks in Public Administration. The results of this work are intended to be a reference for the Public Administration, for the prevention and reaction to damage to people, property, and operation, intentionally caused by external agents, personnel themselves or users. These principles have been applied and validated through a Delphi process in the Administration of the Regional Government of Andalusia in which more than 40 security-related managers have participated.

Keywords

Delphi, Public Administration, Intentional Risks, Homeland Security, Resilience.

INTRODUCTION

The Public Administration is characterized by a great diversity of buildings and facilities for which it is difficult to identify the competencies and responsibilities in terms of security. This is due to the fact that the management scope of security is usually distributed, meeting specialty criteria in the nature of the risks and the impact area, with a very varying degree of development and formalization (Smith and Brooks, 2013; Brooks, 2012). In this way, the scope of industrial risk prevention is generally found highly regulated (ISO 31000), as well as with

legally defined powers and responsibilities. Similarly, a varying degree of legal regulation is found within the scope of information security (ISO 27000), buildings and facilities protection against fire risks, intrusions, external aggression, or against natural events (NCSE-02), such as anti-seismic protection. Likewise, in recent years, the specific legislation has increased at an international level for critical infrastructures protection (Turoff et. al 2016). Most of the specific legislation, that regulates these security areas, is of general application from both the Public Administration and any natural or legal person, according to its scope of application and the definition of responsibilities

These circumstances provide a context for the risk management and the security within the scope of the Public Administration, characterized by (1) a great diversity of the institutional areas with competences concerning issues involved in security risks, (2) a varying degree of definition and development of the organization, powers and responsibilities for security risk management, and (3) a high degree of attractiveness to intentional threats. The Public Administration, like a city inside the city, can be understood as a set of interconnected dynamic systems (Godschalk, 2003).

In spite of the relevance of security within the Public Administration, and of the millionaire budget devoted to the protection of public buildings, there is no scheme that provides an integral global vision of the risks and security management, in all the areas and level within public administrations, and for all the types of risks and impact areas. This is due to the great diversity of existing approaches in the security and resiliency scopes, from different fields (Hernantes et. al, 2017). In order to contribute an initial approximation to this field, in this article, we propose the execution of the Delphi method for the establishment of design principles, and for the definition of the Internal Security Policy within the Public Administration for the reaction and prevention against damage to people, heritage and the operation, intentionally caused by external agents, personnel or users.

The present article takes the following form: In the second section, we will analyze the different types of risks and impact areas against damage, intentionally caused by external agents, personnel or users, to people, heritage or the normal operation within the Public Administration (occupational, infrastructure, heritage, information, aggressions, external risks…). In the third section, the execution of the Delphi method for the establishment of the Internal Security System within the Public Administration will be illustrated with a real case, that of the Andalusian Regional Government, Spain. Both the validation and results of the Delphi method are presented in the fourth section.

BACKGROUND

For the characterization of the actions currently carried out in the field of security, a classification has been used in the Scope of Protection, Type of Threat and Nature of Action dimensions.

Scope of Protection

The actions currently being carried out in the field of security are aimed at the protection of certain types of protectable properties, mainly as a result of the compliance with applicable regulations and legislation.

Protection against threats to the physical security of people and assets

It is the most traditional scope of security protection, aimed at preventing losses and damages in an organization, caused by people or groups whose objective is the appropriation of property, or causing damage to facilities, assets or people (Fisher et al, 2008). This area includes means and systems for prevention, containment, surveillance, detection and action against intrusion, such as perimeter fences, surveillance cameras, access controls, presence or movement detection system and alarm and response systems (ARC). If the risk is significant, it is common for this security function to fall to a specialized area in the organization. It is also common to have authorized external security and surveillance services to perform this function since in certain cases it is required by the legal requirements in the field of private security. In this field, specific national legislation has been developed, driven in recent years by the increase in the global terrorist threat, and including legislation derived from the European directives aimed at protecting critical infrastructures.

Protection against threats to workers' health

This area includes the management of risks to worker's health derived from the conditions and nature of their job: handling of toxic substances, handling of dangerous machinery, extreme environmental conditions, physical overexertion, etc... (ISO 45000). This function usually falls to the human resources area, which may have its own prevention and occupational health service or may have an authorized external prevention system. The methodologies for the evaluation and management of occupational risks are highly developed, and the methods and recommendations praised by the National Institute for Health and Safety at Work are regularly used as a reference.

There exists extensive legislation on occupational health, which establishes precisely the responsibilities and activities of organizations in this area. In this sense, it is compulsory that the organizations have an (own or external) occupational health officer, a Prevention Plan, and prevention service. Legislation and technical standards also cover the scope of protective equipment applicable to each activity. Management standards have also been developed in this area, as well as voluntary certification schemes.

Protection against industrial threats to the personnel, population, and environment

Industrial accidents (fires, explosions, spills, toxic clouds …) have historically caused huge damage at personnel themselves in the facilities, in the environment, and in the surrounding populations. The risk management in this area is aimed at preventing the occurrence of these accidents or minimizing the damage caused (ISO 31000). There exists national legislation in this area which requires the organizations with certain characteristics to have Emergency Plans to respond to possible emergencies. These plans should define the responsibilities for the response to incidents and coordination with external intervention services (firefighters, civil protection, police officers), as well as self-protection actions (evacuation, confinement, threat containment …). The legislation also develops European directives (SEVESO) aimed at protecting the populations against the threat of major accidents. The field of industrial Security also includes the legislation and technical standards applicable to certain equipment and machinery (pressure devices, lifts, fire extinguishers …) which require its certification and periodic verification.

Protection against threats to information security

The development and widespread of the use of communication and information technologies (ICT) in recent times has led to a parallel increase in the volume and sophistication of threats for the integrity of sensitive information for individuals and organizations. Cybersecurity is the practice for the protection of the information and ICT systems against intrusions (hackers) and harmful programs (viruses and malware). It has also been developed management standards in the field of information security and voluntary certification schemes (ISO 27000; ISO 14000).

Protection against threats to essential services for the population

Essential services for the population such as drinking water supply, sanitation, transports or energy supply are subjected to increasing global threats (terrorism, geopolitical tensions…) in an increasingly independent context. In recent years, European and national legislation has been developed for the protection of critical infrastructures which provide these essential services. This legislation establishes responsibilities and mechanisms of analysis, planning, and response to mitigate the risk for these infrastructures, to protect them against threats and to respond to possible incidents which may occur. At the voluntary level, technical standards and certification schemes have been developed for global risk management and its business continuity (ISO 22301; ISO 22320).

Protection against criminal threats

In recent years, the treatment of other types of threats have been formalized such as those which affect the criminal risk of the organizations and workers (compliance) (ISO 19600). National legislation has been developed in this field, as well as international compliance management standards. It is necessary to consider that risks interact with each other so that a criminal risk for workers can become a risk for the continuity of the activity if they limit their

actions to avoid criminal risk. As it is mentioned in the table, the basic regulations may cover more than the protection area.

Type of threat

United Nations Disaster Relief Organization (UNDRO) classifies risks into those caused by natural, human or technological threats:

- Natural: risks of which triggering is not directly caused by human presence or activity, but by climatic and geological factors.
- Human: risks caused or derived from human activities and actions.
- Technological: human risks which derive from technological development and significative use and application of technologies.

On the other hand, public preparedness is considered to be important in the fight against terrorism. So, homeland security needs to give special consideration to threats of intentional origin in Public Administration. Considering the foregoing, the actions in the security area Public Administration could characterized by the criteria of responding to an accidental threat, or an intentional threat, as described in table 1.

Table 1. Types of threat

Type of threat	Description
Accidental	The technological, human and natural threat, of which occurrence is not caused by the intention of groups or individuals to cause damage to protected property.
Intentional	The technological, human and natural threat, of which occurrence is caused by the certain intention of groups or individuals to cause to damage to protected property.

Areas of protection

Security management has also developed in its approach, from its purely instrumental initial conception, in which the organizations provide reactively, ad hoc and isolated responses to emerging security needs. Currently, it is necessary a proactive and systematic approach, with a strategic intention based on the understanding of the context and necessities of stakeholder and using a formalized management system as a tool for developing such strategy. A management system is a group of elements within an organization, which are interrelated or interact to establish policies and objectives, as well as processes to achieve those objectives. Standardized Security Management System models are currently available in various protected areas (Table 2).

Table 2. Standardized Security Management Systems in Protection Area

Model	Area of protection	Type
ISO 45001 Occupational health and safety	Security and health of the workers. It substitutes OHSAS 18001 Standard	Accidental
ISO 22301 Business continuity management	Continuity of essential services	Accidental Intentional
ISO 22320 Social Security. Emergency management	Security and health of the workers Security and health of citizens	Accidental Intentional
ISO 31000 Risk management	A comprehensive model for risk management and incident response in all areas of protection	Accidental Intentional
ISO 55001 Assets management	Model for the asset life cycle management, including its conservation and maintenance	Accidental
ISO34001 Security management system	Protection against internal or external fraud. It is developing	Intentional
ISO 14001 Environmental management systems	Protection of the environmental estate	Accidental
ISO 19600 Compliance management systems	Protection of legal compliance	Accidental Intentional

CASE STUDY

In this case study, the design process of a Comprehensive Risk Management and Security System within the scope of the Regional Government of Andalusia, for comprehensive management of the different types of risks. This system is based on an institutional architecture, a governance system, and the definition of competencies and responsibilities for policy coordination, objectives, strategies and actions in terms of security amongst various government agencies, as well as amongst various operators with competences concerning any risk management area and the security of the Regional Government of Andalusia.

Context

Regional Government of Andalusia is the institution in which the self-government of the Autonomous Spanish Community of Andalusia is organized. It is integrated by the Parliament of Andalusia, the presidency of the "Junta de Andalucía" and the Governing Council. The 2019 budget amount to 34,759 million euros, and it has more than 270,000 direct employees.

Methodology

The research methodology on which this work consists of three sequential phases (Figure 1).

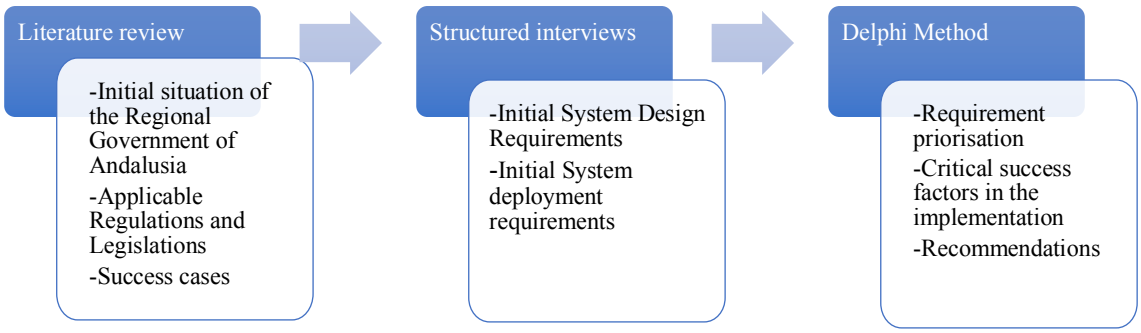

Figure 1. Methodology

The first stage is based on a review of the literature to characterize the initial situation of the security organization in the Regional Government of Andalusia, the main applicable regulations and analysis of success cases and reference of security management at national and international level. In addition, an analysis of the estate inventory has been performed, considering all Central Administrations and Agencies (excluding commercial companies) to define the scope of assets to be protected. As part of this stage, a model of approach to the Internal Security in Public Administration has been proposed, since we have not found in the literature a single approach that allows us to classify the activities at the level of security that is carried out in a Public Administration of the size of the Regional Government of Andalusia. In addition, a glossary of security terms has been compiled. This glossary is based on the main national and international standards, regulations, and legislation.

In the second stage, a series of personal interviews were carried out with 9 interlocutors with responsibilities in different areas of protection in the Regional Government of Andalusia. In these interviews, a wide variety of issues have been posed in order to characterize the current security situation in the Regional Government of Andalusia. This methodology is useful as a means of providing input for an initial approximation of design and implementation requirements of the Andalusian Regional Government's Internal Security System.

In the third stage, the conclusions obtained both from the literature and from the personalized interviews using the Delphi Method were compared. Delphi method is an analytical technique based on the judgment of a group of experts. It consists of an iterative and systematic process aimed at obtaining the opinions, and if possible consensus, of this group of experts. Its main characteristics include anonymity, controlled repetition and statistical treatment of responses. The Delphi method was developed in the Rand Corporation during the 50s (Helmer and Rescher, 1959). This technique was designed to develop a debate independent of personalities. The Delphi method is based on anonymous communication with feedback. Anonymity is required in the sense that no one knows who else is participating. Moreover, judgments are summarized and sent back to the group for further analysis in the form of sequential questionnaires. Processing data in this way help to minimize psychological effects and time demanded in comparison with another group (Linstone and Turoff, 1975; 2002). With the profound impact of the internet on organizational and community planning systems, Delphi it will foster a new age of participation through communication, coordination, and collaboration (Linstone and Turoff, 2010).

Field Work

32 experts have participated in the Delphi process, among all of them there are people responsible and key actors in the future of Internal Security System of the Andalusian Regional Government, such as Technical General Secretariat (TGS) of several Ministries, General Secretariat (GS) of Several Government Delegations, as well as Directorates-General and equivalent departments of key areas for the security field and experts in the field from other Agencies and Directorates-General of the Regional Government of Andalusia. Delphi study had a response rate of 60.37%, which means high participation in the study.

Following the Delphi Methodology, each expert was given a set of principles resulting from the provisional conclusions of the initial study. In addition, a series of open-ended questions were included in which could contribute to relevant aspects not covered in this first round of the Delphi process. In a second round, each expert was given both their response and the group's response so that they could make a comparison and make comments and assessments if they deemed it appropriate. The comments of the entire panel of experts were sent to other participants anonymously so that the rest of the group could establish the degree of agreement on further contributions from the panel of experts.

RESULTS

Design Principles

A first result of the study in the need to establish a Basic Security Management Model for the future Internal Security System for the management of risks caused by international threats of the Regional Government of Andalusia with the following components:

- Security Policy: The definition of the scope of protection, and of overall objectives, principles, and commitment in the security area.
- Government framework: Organization and responsibilities for the definition and deployment of security objects, coordination of actions for risk treatment and analysis, and for the assessment, review, and updating of the security management system.
- "Typological" Analysis of Risk: Identification of the types of threats to the protection area, and "standard methods" for the assessment of the risk associated with the impact and probability of occurrence of the threats.
- Risk treatment: Establishment of criteria and strategies for the treatment of risks, and implementation of the necessary security and protection measures to migrate the risk to an acceptable level.
- Response to incidents: Definition of responsibilities for the identification, notification, and classification of incidents, as well as for the activation and coordination of action plans to respond to the incident.
- Monitoring, Assessment, and Improvement: Monitoring of indicators, security management system audit, and incident response drills, as well as an assessment of the response to an incident that has occurred, they provide information on the effectiveness of the security management system and possible opportunities of improvement.

In a complex organization, as it is the Regional Government of Andalusia, this Base Model may require a Government Framework and deployment according to the different levels and organizational structures. Additionally, the development of the tools for the promotion of Safety Culture in the Regional Government of Andalusia has been established as a priority as a fundamental pillar of the system. Culture is an intangible force behind the measurable and observable that moves an organization to action. Due to the organizational culture has such a profound effect and the behavior of individuals, it should be understood and managed to achieve the desired objectives. The lack of Safety Culture may involve structural risks that are difficult to address. Therefore, any Security System to be promoted by the Regional Government of Andalusia must be rooted in the promotion of the Safety Culture among workers and users of the services.

Other relevant but less important aspects for the panel of experts are:

- Centralization of information: There exists a need to centralize and coordinate information and communications in a complex structure such as de Regional Government of Andalusia in the field of security.
- Resilience: A resilient organization must have the ability to ability to anticipate disruptions, adapt to events

and create lasting value. A resilient system involves the ability to absorb disturbances, respond efficiently and recover from unexpected events. In this sense, the Security System of the Regional Government of Andalusia to be resilient should have the attributes of robustness, redundancyand speed.

- Change management: The success of the implementation of the Security System in the Regional Government of Andalusia also depends on proper management of the possible resistance of a new System, making it easier for the organization itself to accept, support and effectively manage the change.

Keys of implementation

As a result of the Delphi process, the experts on the panel have provided their views on the key aspects of the implementation of each of the Internal Security System's design principles, which we summarize below:

Security Policy, Government Framework, and Management

The experts stress the need to define a Security Policy, including the Management and Government Framework, relevant areas and departments. It is outlined the need to include coordination mechanisms with other existing systems as well as with the national and international security forces. According to the panel, it is essential to consider the particularities of each of administration's activities, especially those with a higher concentration of risks.

According to the participants, the design of the Security Policy must consider all employees and positions of the Regional Government of Andalusia, considering this difference in profiles and responsibilities so that each one can apply the protection mechanisms that are relevant to them. It should also include mechanisms for monitoring, assessment and information management at all levels. The training of those responsible for Security matters is a critical aspect for the success of the implementation as well as the awareness and involvement of workers and users of the services of the Regional Government of Andalusia.

Protection area, Analysis and Risk Treatment

The result of the Delphi process indicates that the threat catalogs need to specifically address the situations of greatest risk exposure. They also count on the contribution of the knowledge of personnel at all levels of the Administration, making catalogs of threats against the administrative structure (services, sections, and negotiations), as well as against the holders of managerial posts in the Regional Government of Andalusia, according to their rank and competences.

According to the panel of experts, the Internal Security System should have communication and dissemination mechanisms that are as broad, complete and close as possible in order to make publish both the catalog of risks that an employee/site faces and the prevention and treatment mechanisms that are applicable. Technical advice on security matters should also be provided on a permanent basis to the institutions.

Responses to Incidents, monitoring, improvement:

The results of the Delphi panel show that, at the level of Incident Response, it is key the specific training of personnel (managers, coordinators, etc.), with special emphasis on those who carry out their activities in centers with high levels of risk. On the other hand, it is outlined the need to perform the Monitoring and Improvement of management indicator implementation in the field of Safety.

It would be essential to establish coordination measures by the Regional Government of Andalusia, but always considering specificities and characteristics of each area, drawing up procedures jointly between the Ministries with competence in the field of Security. In addition, the National Police Unit attached to the Autonomous Community of Andalusia should be involved in the analysis, monitoring, and improvement.

Security culture

Regarding Security Culture, the panel of experts' stresses that the training and awareness in Security are essential to avoid incidents, and also allows for a better reaction in the event of an incident.

For this, it is necessary to involve workers and users, creating Culture but without generating an atmosphere of fear. Such training should begin with that of the management staff of the Ministries and Delegations of the Government and Territorial Delegations.

In order to achieve a greater involvement and awareness by managers, public employees and users, in the opinion

of the panel of experts, it is necessary to improve horizontal and transversal communication channels in the area of security, especially with regard to new recruits who are responsible for safety or who are in charge of buildings or people subjected to relevant risks.

Other key implementations

Regarding the Centralization of Information, the panel proposes to promote the existence of a fluent information channel for those responsible for the different centers, reinforcing and guaranteeing the upward and downward channeling of information. This issue would require common information tools and standardized communication processes.

Regarding the provision of Resilience to the International Security System, the experts indicate that it would be important to guarantee the availability of means and resources in the area of Security, as well as the flexibility and adaptation of the System to the characteristics of each asset, since the risks and implications of these differ according to the context. They also propose the development of tools to analyze unforeseen situations that have caused damage, collecting the appropriate conclusions to prevent or minimize them as far as possible. Resiliency is too often measured against prior natural disasters and climate change is increasing the level of damages above past values so that by replacing what was there and damaged without increasing the resistance/survivability to larger natural disasters is a major decrease in resiliency (Turoff et al., 2018).

Finally, the experts point out that a large part of the success in the implementation of the Internal Security System lies in an adequate Management of Change, whose pillars would be the involvement of the management, awareness campaigns among public employees and users and the training of personnel.

Through adequate communication, the new International Security System should be presented as something positive and not as a new workload and responsibilities, reflecting the need for its proper development and the benefits of its implementation.

Model base

The conclusions of the panel of experts firstly highlight – with a level of agreement of 4.71 on the scale of 5, where 5 suppose "total agreement" – the need to establish a global governance framework and management of security in the face of international risks at the level of the Regional Government of Andalusia. This government framework should allow for the definition and effective and coordinated deployment of comprehensive security policies, as well as those established in each specific area of protection. As we mentioned in the methodological section, this panel of experts have key actors and responsible people in the future of Internal Security System of the Regional Government of Andalusia such as SGT of various Ministries, GS of some Government Delegations as well as Directorates-General and equivalent departments of key areas for the field of security and experts in the field from other Agencies and Directorates-General of the Regional Government of Andalusia.

A series of principles are also established for the design of an Internal Security System in the event of international threats to the Regional Government of Andalusia. A first element to be included in the design is the establishment of a Base Model for the Management of Internal Security which elements and interrelations are expressed in figure 2.

Some key properties to include in the design of the System for the correct functioning of this Base Model would be the Security Culture, the Centralization of Information, the work for Resilience and a Change Management design.

At the implementation level, key factors are considered:

- Coordination with other existing systems and at different levels of management.
- Management commitment.
- Communication with everyone involved in the system.
- Awareness-raising at all levels, including users.
- Training as a key to promoting a Culture of Security and Change Management.

In this sense, the panel of experts stress that the processes of design and implementation of the new Internal Security System must consider developments in the field, requiring the active participation of the various Ministries, Management Centers, and Entities of the Andalusian Regional Government, through the appointment of their heads or coordinators. It is essential to be able to transmit the advantages and benefit of the new System, as well as to plan the required resources for launching it and establish a well-defined roadmap for its implementation.

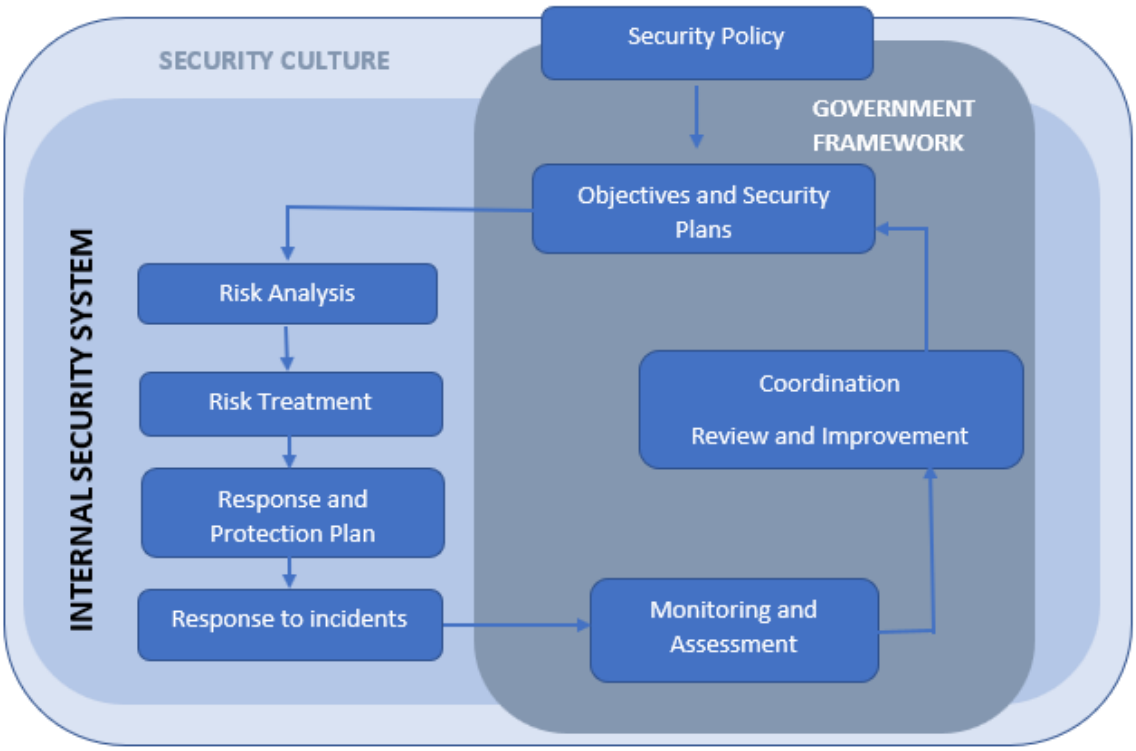

Figure 2. The relationship among elements of the Base Model for Security Management

It is also necessary the communication and the training at all levels un matters of safety, fundamentally regarding the rights and obligations derived from own and third parties' actions in the use of material elements and the use of public buildings.

CONCLUSIONS

In this article, a Delphi approach has been proposed for the establishment of design principles of a Comprehensive Risk Management and Security System in a large Public Administration. With this system, we have aimed to provide a global approach to carry out planning, prevention, protection, reaction, assessment and improvement activities, as well as the coordination amongst the various kinds of agents involved in terms of security against international threats.

One early conclusion is the transversal nature of the security within the Public Administration. This matter makes the integration and identification of a Comprehensive Risk Management and Security System with other possible high-level shortcomings within the organization with competences concerning security, respecting the identity of the rest of the systems despite defining coordination mechanisms amongst one of them, be one of the main challenges when it comes to developing a Comprehensive Risk Management and Security System

A second conclusion is the adequacy of the Delphi method to define a Comprehensive Risk Management and Security System. As it has been stated before, these systems have various kinds of ramifications and interactions with all the Public Administration structure. Due to the suitability of the Delphi method for dynamic planning in episodes of high uncertainty, this technique has shown itself to be added value in the process by the Administration for its execution. The best indication is that, based on the established principles, the regulatory support for the assurance of the governance of the Comprehensive Risk Management and Security System in a Public Administration has been developed.

ACKNOWLEDGMENTS

We want to express our gratitude to the authorities and officials of the Administration of the Junta de Andalucía who, always interested in the continuous improvement of the facilities' security, have collaborated in this research.

REFERENCES

Brooks, D.J., 2012. Corporate security: Using knowledge construction to define a practising body of knowledge. *Asian Journal of Criminology,* http://dx.doi.org/10.1007/s11417-012-9135-1.

Fischer, R.J., Halibozek, E., Green, G., 2008. Introduction to Security, eighth ed. Butterworth-Heinemann, Boston.

Godschalk, D. R. (2003). Urban Hazard Mitigation: Creating Resilient Cities. Natural Hazards Review, 4(3), 136–143. https://doi.org/10.1061/(ASCE)1527-6988(2003)4:3(136).

Helmer, O., and Rescher, N. (1959). On the epistemology of the inexact sciences. *Management Science*, 6(1), 25–52.

Hernantes, J., Labaka, L., Turoff, M., Hiltz, S.R., Bañuls, V.A. (2017) Moving forward to disaster resilience: Perspectives on increasing resilience for future disasters. *Technological Forecasting and Social Change*, 121, pp. 1-6.

ISO 14001: Environmental management systems. https://www.iso.org/iso-14001-environmental-management.html.

ISO 19600: Compliance management systems. https://www.iso.org/standard/62342.html.

ISO 22301: Business continuity management. https://www.iso.org/standard/50038.html.

ISO 22320: Social Security. Emergency management. https://www.iso.org/obp/ui/#iso:std:iso:22320:ed-2:v1:en.

ISO 27000: Information security management system. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

ISO 31000: Risk management. https://www.iso.org/iso-31000-risk-management.html.

ISO 34001: Security management system. https://www.iso.org/obp/ui/#!iso:std:61588:en

ISO 45001: Occupational health and safety. https://www.iso.org/iso-45001-occupational-health-and-safety.html

ISO 55001: Assets management. https://www.iso.org/standard/55089.htm

Linstone, H.A., and Turoff, M. (Eds.), The Delphi method: techniques and applications, Addison-Wesley, Reading, Mass, 1975. (Available online at http://is.njit.edu/turoff).

Linstone, H.A. and Turoff, M. (2011) Delphi: A brief look backward and forward, *Technological Forecasting and Social Change*, 78 (9), pp. 1712-1719.

Real Decreto 997/2002, de 27 de septiembre, por el que se aprueba la norma de construcción sismorresistente: parte general y edificación (NCSR-02).

Smith, C. L., & Brooks, D. J. (2013). Security Science: the theory and practice of security. Butterworth-Heinemann, Boston [978-0123944368].

Turoff, M. Bañuls, V. Ramírez de la Huerga, M. (2018) Hurricanes Send Signals for the Future of Emergency Preparedness. *Proceedings of the ISCRAM 2018 Conference*, Rochester, US.

Turoff, M., Bañuls, V., Hiltz, S.R., Plotnick, L., and Ramírez de la Huerga, M. (2016) A Collaborative Dynamic Scenario Model for the Interaction of Critical Infrastructures. *Futures*, Volume 84, Part A, November, Pages 23–42.