Expert technical evaluation model for modeling and monitoring services of Technology Information and Communication services in a Social Security Institution of the Federal Public Administration

Modelo técnico experto de evaluación para servicios de modelado y monitoreo de servicios de Tecnología de Información y Comunicación en una Institución de Seguridad Social de la Administración Pública Federal

ZAMORA-SOTELO, Carlos*†

Universidad Iberoamericana, Prolongación Paseo de la Reforma 880, Lomas de Santa Fe, Ciudad de México.

ID 1st Author: *Carlos, Zamora-Sotelo*

DOI: 10.35429/JPE.2020.7.4.29.38 Received September 20, 2020; Accepted November 13, 2020

Abstract

Social security services are transcendental worldwide activities with significant impact on critical variables for the rest of the productive apparatus and consumption of a nation. The indicators of this category are always significant to locate the level of development and social consciousness of a country. Expert opinion assessments of the modeling and monitoring of Information Technology and Telecommunications services are intended to provide an assurance initiative as an external control system intended to guarantee the organizational continuity of Information Technology services, and serve as a countermeasure to guarantee the goals and objectives of public organizations related to social security services that are to be provided to a significant portion of Mexico's citizens. This study focuses on one of the major social security institutions in Mexico, which uses the capability assessment model and the specifications of best practices related to assurance model framework provided by COBIT.

Resumen

Los servicios de seguridad social son actividades trascendentales a nivel mundial con impacto significativo en variables críticas para el resto del aparato productivo y de consumo de una nación. Los indicadores de esta categoría son siempre significativos para ubicar el nivel de desarrollo y conciencia social de un país. Las evaluaciones de opinión de expertos del modelado y monitoreo de los servicios de Tecnología de la Información y Telecomunicaciones tienen como objetivo proporcionar una iniciativa de aseguramiento como un sistema de control externo destinado a garantizar la continuidad organizacional de los servicios de Tecnología de la Información, y servir como una contramedida para garantizar las metas y objetivos del público. organizaciones relacionadas con los servicios de seguridad social que se brindarán a una parte significativa de los ciudadanos de México. Este estudio se centra en una de las principales instituciones de seguridad social en México, que utiliza el modelo de evaluación de capacidades y las especificaciones de las mejores prácticas relacionadas con el marco del modelo de aseguramiento proporcionado por COBIT.

Citation: ZAMORA-SOTELO, Carlos. Expert technical evaluation model for modeling and monitoring services of Technology Information and Communication services in a Social Security Institution of the Federal Public Administration. Journal-Public Economy. 2020. 4-7: 29-38

* Correspondence to Author (email: czamora@conseti.com)
† Researcher contributing as first author

Introduction

Social security services in Mexico have always been entirely located in the fields of economics, as well as administration and politics, which, together with education, represent the two most critical sectors of the economy for the federal administrations, and form a central point for the mobilization of interests and a fundamental aspect to structure the offer of the federal government. Social security services that provide services to the population with the capacity of economic resources for payment [1] are based on World Bank studies and other research [2]. The development and access to Information Technologies to improve the results of social security services to the population is the factor with the greatest incidence on welfare that every State should provide the population.

This study primarily describes the operational model of modeling and monitoring services of Technology Information and Communication services in a Social Security Institution of the Federal Public Administration of Mexico. This model is intended to be a response to the results of the "General Report of the Public Account 2014” [3], where the results of the evaluation on Information and Communication Technologies (ICT) of the Institution—which is the subject of this study—issued a maturity capacity assessment of level 2 (repeatable), thus implying a high risk in the continuity of the services. The study’s secondary goal is to propose an external control system to "evaluate and monitor" the functioning of the model as a response to the ICT assurance framework proposed by the assurance reference framework established in COBIT [4].

Analysis Factors

The study of the operational model of the modeling and monitoring services of information and communications technology services consisted of modeling the schema of service operations in order to identify the components that make up the model, evaluate their operation and deployment activities, evaluate the technology to ensure the availability of the assets involved in the model, as well as the risk factors that affect the operation of the model, along with the measures that must be adopted by the institution to achieve compliance with the objectives and benefits established in the specification of the services involved.

The social security institution enabled the modeling of the critical computer applications that would allow the Institute to correctly establish and unify the catalog of ICT services in order to carry out the identification, definition, knowledge transfer, and maintenance of the components that make up the offered services. Likewise, it would allow for the discovery and modeling of the enabling elements of ICT (processes, people, applications and infrastructure) to correctly identify the ICT elements that support the critical applications of the Institute. With this modeling information, the managed services are linked with the critical applications of the institution, along with all the elements that support and enable said services.

The objectives of the application of the model were:

- Describe the services offered in a comprehensible manner for non-specialized personnel, placing special care in avoiding the use of technical language.
- Create guidelines to guide and direct the internal and external clients of the Institution.
- Collect other policies and conditions for the management of critical ICT services, as well as the responsibilities associated with each of these.
- Register the current clients of each critical ICT service.
- Availability of the central service desk and all personnel who have direct contact with customers.
- Increase the confidence of the Institution when it comes to renewing or extending the contracts for the providing of services.
- Identify those responsible for each service to avoid “management vacuum” situations, in which the client does not know who to turn to for advice.

Processes Involved:

Following the principles of the General Application of Information Technologies, Communications, and Information Security Administrative Manual (*MAAGTICSI* for its Spanish initials) [5] and ITIL v3 best practices, I considered the following processes:

1. Incidents
2. Requirements
3. Levels of Service
4. Catalog of Services
5. Assets and Configurations
6. Events
7. Availability
8. Problems
9. Changes
10. Knowledge
11. Suppliers
12. Budget
13. Capacity
14. Demand

For the processes aligned to *MAAGTICSI*, and heeding the best practices of ITIL v3, working meetings were conducted with the people in charge of the DTED and a team of specialists from Neixar, and the following are the requirements identified:

The recollection of information to detect the existing processes operating under the umbrella of the Director of Institutional Technology, the identification of relationships between the critical applications of the Institution, the identification of responsible parties of the operation, and the service levels of the critical applications.

The processes are then designed with the information obtained, along with the definition of the scope, objective, roles and responsibilities, levels of service, integration with other processes, flow diagram of the process, and other particular characteristics thereof.

The processes were delivered according to the phases that were established in the annex, with only a couple processes being switched. Once the Head of Planning of Services approved the processes, they were assigned according to the structure defined by the Institution for the management of the *MAAGTICSI* processes, according to the following sub-processes:

- Services Catalog Management
- Demand management
- Budget Management
- Availability Management
- Capacity Management
- Service Level Management
- Vendor Management
- Configuration Management
- Incident Management
- Service Request Management
- Problem Management
- Change Management
- Event management
- Knowledge Management

The operational model was then established as follows:

Initial component of the model

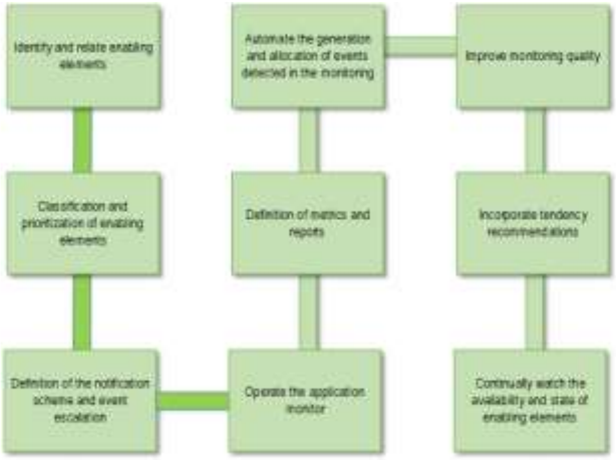
Identify and relate enabling elements
Automate the generation and allocation of events detected in the monitoring
Improve monitoring quality
Classification and prioritization of enabling elements
Definition of metrics and reports
Incorporate tendency recommendations
Definition of the notification scheme and event escalation
Operate the application monitor
Continually watch the availability and state of enabling elements

Figure 1 Initial Component of the Model
Source: Personal Collection

Model complements

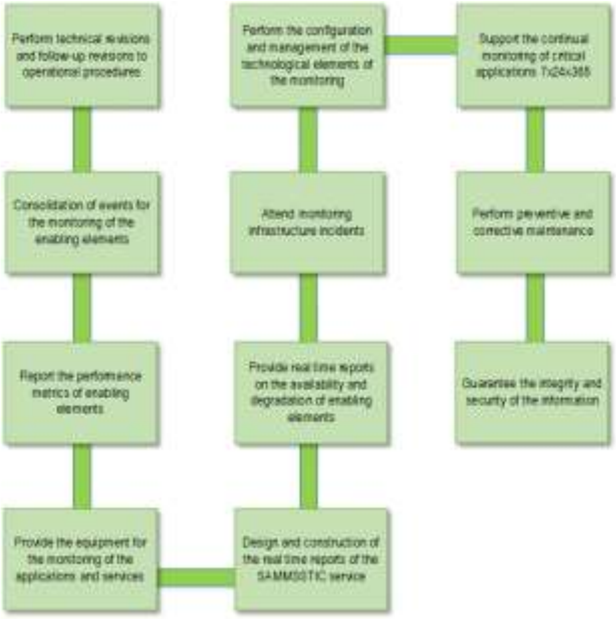
Perform technical revisions and follow-up revisions to operational procedures
Perform the configuration and management of the technological elements of the monitoring
Support the continual monitoring of critical applications 7x24x365
Consolidation of events for the monitoring of the enabling elements
Attend monitoring infrastructure incidents
Perform preventive and corrective maintenance
Report the performance metrics of enabling elements
Provide real time reports on the availability and degradation of enabling elements
Guarantee the integrity and security of the information
Provide the equipment for the monitoring of the applications and services
Design and construction of the real time reports of the SAMMSSTIC service

Figure 2 Model Complements
Source: Personal Collection

The services administered by the model also acknowledge the following components:

1. Process framework aligned to *MAAGTICSI* and ITIL v3 best practices.

2. Modeling and monitoring of the Institutions' critical applications and ICT services.
3. Central Service Desk enabling.

The Institution also required the creation of a Central ICT Service Desk that would function as the only contact point to attend to the requirements and anomalies presented in the Institution's critical applications.

The Institution deployed the required software tools with along with their accompanying licensing and support contracts from the service provider; the IT Service Management platform is contained within these tools. This platform is used for the operation of the Central Service Desk, which provides assistance and support for personal computer equipment issues—these computers are provided via the Personal Computer Equipment Administration Service (SAECP) contract. These tools and components will enable and strengthen the capabilities of the operation of the Central Service Desk, incorporating a model of integration with specialized suppliers to monitor follow-ups and solving failures or service requests for ICT (which are under the responsibility of the different vendors).

This will allow the correct measuring of the service levels and guarantee the *availability and continuity* of the services. Likewise, the automation of follow-up and support processes of the different critical applications of the Institution would be implemented, thus guaranteeing the adherence to *MAAGTICSI* principles and ITIL v3 best practices, as well as strengthening the catalog of services of the Technology Department. Once the model is implemented the Institution would be able to:

- Implement and automate a bidirectional integration model with the specialized service desks of the ICT service providers, which would allow for maintaining a unified workflow for the follow-up requests of the users of the Institution. This would allow for the monitoring and measurement of service levels related to the follow-up and resolution of these requests, and supporting the identification of the root cause of events that affect or degrade the availability and continuity of critical computer applications. The number of specialized service desk integrations needed would be based on current contracts.

- Define and implement the Central Service Desk management processes, incorporating all best practices in order to comply with *MAAGTICSI*, ITIL v3 and the regulations of the Institution.

- Enable a logical and conceptual design of a unified CMDB, which allows the Institution to identify and update the information of the configuration elements of the Critical Applications, which are managed by the different vendors, in an automatic manner. The implementation of the CMDB will be in the technological platform owned by the Institution.

- Maintain an updated Catalog of ICT Services, which allows for the management of the relationships and interdependencies of the configuration elements, both with the services provided through third parties, as well as with the management and operation processes of the Central Service Desk.

- Define, enable and automate the metrics and indicators that will be used in the reports that will allow the Institution to monitor compliance of the service levels established with the various vendors.

The second component of the case study in this research implements an external control system to "evaluate and monitor" the operation of the model as a response to the ICT assurance framework supported by the assurance framework established in CoBIT for Assurance®.

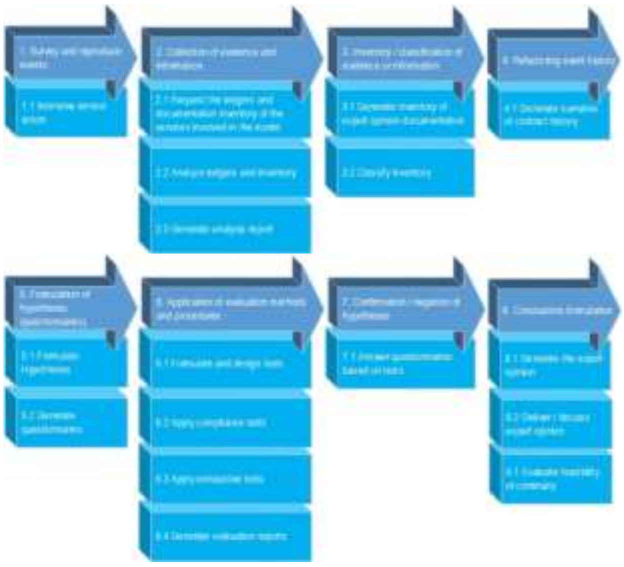
2.3 Generate analysis report
3.2 Classify inventory
5.2 Generate questionnaires
6.1 Formulate and design tests
6.2 Apply compliance tests
6.4 Generate evaluation reports
8. Conclusions formulation

Figure 3: External Control System based on CoBIT for Assurance
Source: Personal Collection

1. **Survey and reproduce events:** A thorough review of all the different elements that make up the entire execution history of the services contained in the service model will be performed. This will allow for a subsequent replay, which will be used for a complete evaluation of the service execution.

1.1. **Interview service actors.** Integrate and document interviews with the different parties involved in the contract established by the organization's contract provider, as well as those responsible for the processes and services impacted by it, understanding their point of view regarding the execution and achievement of the objectives.
Inputs: Environmental factors, contract subject to assurance, IT needs, organization needs, organization strategy, policies and organizational procedures, requirements, IT goals, goals of the organization, expectations of the stakeholders.
Tools: Expert judgment, interviews with stakeholders, review of the IT governance framework.
Outputs: Documentation of stakeholder requirements, documentation of interviews with suppliers.

2. **Collection of evidence and information:** Gather all documents that make up the development of the target of the contract in accordance with the deliverables and reports of the services included in the model

2.1. **Request the ledgers and documentation inventory of the services involved in the model.** Gather the technical, administrative and legal reports generated during the supervision service from the organization, as well as documents that are used as support in the development of deliverables, compliance with the objectives, and scope of the assurance contract.
Inputs: Technical report, administrative ledgers, legal ledgers, documentation of the services contemplated in the model, deliverables, project management documents, reports of expert opinions.
Tools: Documentation analysis and information exploitation.
Outputs: Inventory of classified, identified and structured documentation.

2.2. **Analyze ledgers and inventory.** Evaluation of the different documents requested in point 2.1 and each of them will be classified according to corresponding matches
Inputs: Project ledgers, documentation inventory.
Tools: Documentation analysis and information exploitation.
Outputs: Document correspondence list for the services subject to assurance.

2.3. **Generate analysis report.** Generate a document where the different classified elements are listed, as well as their corresponding degree of compliance with the services included in the model.
Inputs: Corresponding documentation for the assurance contract, project ledgers, documentation inventory
Tools: expert analysis techniques.
Outputs: Analysis documentation.

3. **Inventory / classification of evidence or information:** Perform inventory of documents belonging to the assurance service.

3.1. **Generate inventory of expert opinion documentation.** Gather each of the documents that are subject to the assurance contract, which will support the development of deliverables, meeting of objectives and scope, technical, legal and administrative terms, and enabling the generation of an inventory of different documents developed in the assurance service. ***Inputs:*** Document analysis, project ledgers, documentation inventory.
Tools: Information analysis, tools and techniques of auditing and field expertise.
Outputs: Inventory of all documentation pertaining to the contract.

3.2. **Classify inventory.** Classify the inventory developed in point 3.1 it according to the characteristics of its elements, to facilitate its manipulation at the time of evaluation.
Inputs: Inventory of all the documentation related to the service model
Tools: Information analysis, data management techniques, tools and techniques of auditing and field expertise.
Outputs: Identified, classified, and structured inventory of all documentation related to the contract.

4. **Refactoring event history:** Create a narrative based on the documentation and evidence available in regards to the assurance contract.

4.1. **Generate narrative of contract history.** Generate a chronologically arranged ledger, taking into account the administrative, technical and legal elements, and establish the events that were developed over course of the contract until the moment of the assurance service.
Inputs: Identified, classified and structured inventory of all documentation related to the contract.
Tools: Information analysis, data management techniques, tools and techniques of auditing, field expertise, ledger format.
Outputs: Ledger document taking into account the administrative, technical and legal elements.

5. **Formulation of hypotheses (questionnaires).** Generate the inductive, deductive and necessary statistical hypotheses necessary for the evaluation, and subsequent conclusion.

5.1. **Formulate hypotheses.** State the different hypotheses that, through their verification, will allow an evaluation of the fulfillment of the service model.
Inputs: Factual history, documentation inventory, international standards, internationally accepted best practices, contract subject to assurance, audit principles.
Tools: Document analysis and expert judgment.
Outputs: Hypotheses raised

5.2. **Generate questionnaires:** Formulate the questions that allow the verification of the hypotheses raised in point 5.1
Inputs: Suggested hypotheses, documentation inventory, international standards, internationally accepted best practices, contract subject to assurance, audit principles, document inventory, factual narrative.
Tools: Expert judgment, formulation of questions.
Outputs: Questionnaires for hypotheses proofs.

6. **Application of evaluation methods and procedures.** Review the mechanisms used for the design of the exhaustive tests, their compliance, and their execution, thus allowing for the generation of the findings report.

6.1. **Formulate and design tests.** Generate mechanism and design of compliance and exhaustive tests that allow the evaluation of each of the hypotheses.
Inputs: Hypothesis raised, questionnaires for the verification of hypotheses, international standards, internationally accepted best practices, contract subject to assurance, audit principles, factual narrative.
Tools: Expert judgment, analysis of documentation.
Outputs: List of compliance and exhaustive tests to be executed.

6.2. **Apply compliance tests.** Determine the existence of evidence and deliverables that support the fulfillment of the service model.
Inputs: Selection of compliance tests to be applied, international standards, internationally accepted best practices, contract subject to assurance, audit principles, products / deliverables and documentation derived from the contract, inventory of documents, narrative of facts.
Tools: Interviews, document reviews, product / deliverable reviews, information analysis.
Outputs: Results of compliance tests.

6.3. **Apply exhaustive tests** Evaluate the degree of compliance of each of the deliverables and obtain evidence, according to the characteristics determined within the service model, and that allow for the generation of its evaluation.
Inputs: Selection of exhaustive tests to be applied, international standards, internationally accepted best practices, contract subject to assurance, audit principles, products / deliverables and documentation derived from the service model, document inventory, factual narrative
Tools: Interviews, document reviews, product / deliverable reviews, information analysis.
Outputs: Results of exhaustive tests.

6.4. **Generate evaluation reports.** Document all findings, supported by the exhaustive and compliance tests.
Inputs: Results of compliance tests, results of substantive tests, international standards, internationally accepted best practices, contract subject to assurance, audit principles.
Tools: Information analysis and result graphs
Outputs: Reports of evaluation results.

7. **Confirmation / Negation of hypothesis.** Statements on the hypotheses, thus determining if each one of the proposals is either true or false.

7.1. **Answer questionnaires based on tests.** Respond to the hypotheses generated through the questions posed within the questionnaires associated to each of these, based on the report of the tests generated in point 6.4.
Inputs: Questionnaires for the verification of hypotheses, reports of evaluation results, contract, contract subject to assurance, principles of audit, inventory of documents, narrative of facts.
Tools: Report analyses.
Outputs: Questionnaires for the verification of resolved hypotheses.

8. **Conclusions Formulation.** Generate statements of compliance through the documents of
the expert opinion, including the technical, legal and administrative aspects.

8.1. **Generate the expert opinion.** Generate the reports where the compliance of each one of the different hypotheses is declared, classifying the legal, administrative and technical aspects of each one.
Inputs: Questionnaires for the verification of hypotheses solved, contract subject to assurance, audit principles, inventory of documents, narrative of facts.
Tools: Tools and techniques of auditing, documentation and information analysis.
Outputs: expert technical opinion.

8.2. **Deliver / discuss expert opinion.** Present the results of the administrative, legal and technical reports with the different stakeholders on behalf of the organization: those responsible for the processes affected by the contract and the vendor. Identify the elements presented therein and, if
required, specify what necessary steps need to be taken for there to be an agreement by each of the parties.
Inputs: Expert technical opinion.
Tools: Reviews.
Outputs: Comments by interested parties, expert technical opinion adjusted.

8.3. **Evaluate the feasibility of continuity.** Based on the resulting opinions from the process of point 8.2, evaluate the opportunity to continue with the contract and achieve the objectives and benefits as planned; and, if not, inform all parties so that the necessary actions are taken.
Inputs: Adjusted expert technical opinion, comments from stakeholders, procedures and organizational policies, environmental factors, applicable regulations, international standards, internationally accepted best practices, contract subject to assurance.
Tools: Expert judgment, information analysis.

Outputs: Feasibility of continuity of the model.

8.4. **Generate technical opinion of continuity.** Determine the activities that will be carried out in order to complete and fulfill the assurance contract and achieve fruition.
Inputs: Feasibility of continuity.
Tools: Expert judgment.
Outputs: Continuity technical report.

The expert and technical opinions have strict adherence to the methodology, standards and frameworks included in the target of the service model and technical proposals of the vendors, therefore, in the annex and technical specifications of the service, the aforementioned points must be specified.

Using a representative sampling technique, satisfaction surveys and questionnaires of all parties involved were assessed, and the result was that 95% of the products / services defined within the scope of the contract were delivered.

All parties involved must carry out the handling of evidence and official documentation, which reflects communication during the development of the delivery of services, with impeccability and formality in accordance with the approved communication plan. Availability of the logs, databases and applications that allow for the assurance, must be available in order to access the necessary information to validate the SLA.

The Institution involved has implemented systems and external control processes through third-party outsourcing mechanisms for the technical supervision of contracts with great technical and logistical complexity. However, these external control systems contain traditional compliance mechanisms for compliance evaluation and supervision of activities by trained personnel to perform control verifications, better known as assurance checklists. These personnel do not necessarily have the technical skills, experience and knowledge to be able to carry out a complete and sufficient evaluation of the technical compliance and good functioning of the assets that they are supervising.

In this sense, the external control system used for the development of this case study offers an action protocol with four critical success factors that demonstrate its usefulness for the management of the evaluated service model:

– The participation of specialized experts in the review of operations and technical compliance showed that knowledge and experience is important when detecting deviations and breaches by service providers of the institution.

– The application of the evaluation and certification protocols of the service model gave the Institution the possibility of managing the service model in strict compliance with its original mandates, thereby allowing for an effective rendering of accountability on the use of public resources.

– The evaluation and certification protocols included the participation of specialists to provide certainty and transparency to the process of accountability at the beginning, and at the end, of the application of the assurance system.

– It Allowed the authorities of the institution to have an application tool that allowed the following capabilities at all times:
– Know the risks and critical success factors of the contract
– Know the status of compliance and service delivery as a result of technical evaluations carried out during the development of the provision of services
– Gather, classify, and assign an electronic ID number to all the technical, administrative and legal documentation of the project for its later integration into electronic storage media, eliminating the use of physical papers.

Results

Existing baselines prior to the application of the expert services model to the modeling and monitoring services of Information Technology and Communications services in the Institution:

- Never had an assurance framework-based evaluation system been applied to the technology services of the Institution.
- Compliance with the objectives and benefits of the services had never been verified through any method, tool or procedure.
- No action protocol had ever been executed to verify, validate or certify compliance with the specifications of the service model, as well as its conditions and specifications.
- Prior to the application of the service model, no civilians had ever been invited to witness the transparency and accountability of the exercise of the public budget pertaining to any contract related to ICT.
- Before the application of the expert technical evaluation model, no deviations were detected in the compliance of the service model by the officials involved with the functions of operating and administering the model of institutional services.

The application of the external control system—known as the Pakal System—in the CONACYT resulted in the following scenarios:

- Verification of compliance with objectives and benefits established in the service model.
- The establishment of a baseline of process capabilities, people and technology involved to improve the quality and maturity of the services involved.
- The application of technical and legal action protocols for the validation and certification of compliance, through the instrument known as “expert opinion of evaluation and judgment” by application of the scientific method.
- Civilians were summoned, through the representation of academics and scientists from two universities, one public and one private, to validate the results through a closing protocol
- During the application of the evaluation model, eighty-six deviations were detected that were corrected during the development of the delivery of the services, contributing to the achievement of the objectives and benefits specified in the justification thereof.
- The service model administrator evaluated and verified the benefits provided by the expert technical evaluation model by providing all the elements of information and action protocols needed to obtain compliance and certify the achieving of the objectives and benefits established in the justification of outsourcing for the benefit of the users and the Institution.
- The experience of applying the expert technical evaluation model to the services experienced by the contract administrator indicates approval and satisfaction of the fulfillment of the objectives for which they were implemented.

Conclusions

The design and application of the expert technical evaluation model *to the modeling and monitoring services of the Information and Communication Technologies services in the Social Security Institution,* demonstrates that it is an adequate tool to verify the hypotheses raised in this research. This in the sense of verifying the usefulness that this model can serve as an instrument for governance in terms of ICT services and procurement for a federal government agency of Mexico.

The results of the study show that the expert technical evaluation model fulfills the objectives and purposes of the institution for which it was applied to. The aforementioned model works correctly for the purposes that it was designed and constructed for, and that it is very useful to the institution for the purposes of transparency and accountability before the law, as expressed by public officials of the entity.

The main contribution and innovation of the expert technical evaluation model is the evaluation protocol that was established, which allows for the detection of omissions and deviations in compliance with the specifications of the contract. This protocol generates observations and recommendations for immediate settlement and correction by all those involved.

The expert technical evaluation model is an external control system that establishes, through a method and action protocols supported by regulations, an intervention model to supervise and ensure compliance with the provisions of the law through expert evaluations through the generation of expert opinions.

The hypothesis of the research study raises the possibility of the model being used as a tool that contributes—through methods, processes, and technological tools—to the compliance of norms, dispositions, and laws in matters of acquisitions and responsibilities of the public administration. The model, being an external control system, is a set of elements that affects the supervision, surveillance and assurance of compliance with standards and legal provisions. The hypothesis does not propose that its main objective is to verify the impact that the system has on the behavior of public servants when the external control system is applied: this area of study can be the subject of another research project.

References

[1] Escobar, Agustín *La Calidad de la Rendición de Cuentas: Transparencia y Acceso Efectivo al Seguro Popular*. 2012.

[2] Organización para la Cooperación y el Desarrollo Económico (OCDE). *Panorama de la salud (Health at a glance)*. 2011.

[3] Informe General Cuenta Pública 2014, *Estudio General sobre las Tecnologías de Información y Comunicaciones en la Administración Pública Federal, Anexo 6*, Cámara de Diputados, México. 2015.

[4] ISACA. (s.f.). CoBIT 5 for assurance.

[5] The *MAAGTICSI* is a manual that establishes the administrative dispositions regarding information technology and communications, and information security, which must be followed by the dependencies and entities of the federal public administration (APF), as well as the Attorney General's Office of the Republic of Mexico. The manual defines and approves the processes that govern the operation of the ICT and information security units of the Federal Public Administration institutions in order to increase the operational efficiency and improve the delivery of services to society.
.