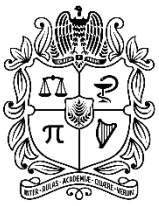


UNIVERSIDAD
NACIONAL
DE COLOMBIA

Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001

Juan Pablo Berrío López

Universidad Nacional de Colombia

Facultad de Minas, Departamento de Ciencias de la Computación y la Decisión

Medellín, Colombia

2016

Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001

Juan Pablo Berrío López

Tesis de investigación presentada como requisito parcial para optar al título de:

Magister en Ingeniería – Ingeniería de Sistemas

Director (a):

MSc., Gustavo Adolfo Pérez Zapata

Línea de Investigación:

Seguridad de la información

Universidad Nacional de Colombia

Facultad de Minas, Departamento de Ciencias de la Computación y la Decisión

Medellín, Colombia

2016

A quienes me enseñaron que el amor, el trabajo y el conocimiento, deben ser parte de mi existencia y decisión: Mis Padres.

A mi novia, por su apoyo y ánimo que me brinda cada día para alcanzar nuevas metas tanto personales como profesionales.

Agradecimientos

A mis padres y mi hermano, por su apoyo incondicional en la lucha por alcanzar mis metas, por su amor y esmero por mi bienestar.

A mi novia Yury, por brindarme su amor, su cariño, y contagiarme de su disciplina y tenacidad.

Al profesor Gustavo Pérez, director de este trabajo, por sus valiosos aportes y orientación. Gracias por la confianza ofrecida siempre.

A mi jefe, amigo y maestro, Eleazar Carmona, por su constante acompañamiento y valioso conocimiento que me ha aportado en toda esta carrera.

Al profesor Jovani Jiménez, por su carisma diligente y voluntad de enseñar siempre.

A los expertos que participaron en el desarrollo de la tesis, compañeros de trabajo y amigos.

Resumen

La información es un activo valioso para las organizaciones, y la protección de esta, un objetivo prioritario para la operación del negocio. La información está cada vez más disponible en ambientes interconectados lo que genera un riesgo a posibles vulnerabilidades y amenazas. Estos riesgos hacen indispensable contar con mejores prácticas de seguridad de la información para minimizar los daños y asegurar la continuidad del negocio. El estándar ISO/IEC 27001 se desarrolló con el objetivo de proporcionar requisitos de control para establecer, implementar, mantener y continuamente mejorar los sistemas de gestión de seguridad de la información (SGSI) de una organización. Los SGSI son un enfoque sistemático para el manejo de información confidencial de las organizaciones con el fin de que esta permanezca segura. La mayoría de las metodologías analizadas evalúan los controles de seguridad de la información de manera muy subjetiva lo que conlleva a una inadecuada implementación de los SGSI. Con el fin de abordar este problema, en esta tesis de maestría se propone una metodología que permite evaluar y posteriormente seleccionar controles de seguridad clave con base en la opinión de expertos usando el método Delphi. La metodología propuesta está basada en los requisitos de control del estándar ISO/IEC 27001.

Palabras clave: ISO/IEC 27001, SGSI, Seguridad de la Información, Activos de Información, Auditoría.

Abstract

Information is a valuable asset for organizations and its protection is one the main objectives for business operation. Information is increasingly available in interconnected environments, which can lead to potential risks such as system vulnerabilities and threats. It is necessary to implement best information security practices for minimizing such risks. ISO/IEC 27001 standard is developed in order to provide control requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) of an organization. ISMS is a systematic approach to manage confidential information of organizations in order to keep it secure. Most of the analyzed methodologies subjectively evaluate information security controls, which lead to inadequate implementation of the ISMS. In order to address this problem, in this M.Sc. Thesis We propose a methodology for evaluating and selecting key security controls based on expert's opinions by using the Delphi method. The proposed methodology is based on the control requirements of the ISO/IEC 27001 international standard.

Keywords: ISO/IEC 27001, ISMS, Information Security, Information Assets, Audit.

Contenido

Pág.

Resumen ..... **V**

Lista de figuras ..... **IX**

Lista de Tablas ..... **XI**

Lista de Símbolos y abreviaturas ..... **XII**

Introducción **1**

1. Marco Teórico **3**
1.1 Modelo de Deming 3
1.2 SGSI – Sistema de gestión de seguridad de la información 6
1.3 ITIL- Information Technology Infrastructure Library 14
1.4 COBIT – Control Objectives for Information and Related Technology 17

2. Problema y justificación de la investigación **23**

3. Revisión de literatura **25**
3.1 A New Method for the Identification of Proactive Information Security Management System Metrics 25
3.2 Evaluating the effectiveness of ISO 27001:2013 based on Annex A 26
3.3 Physical and logical security risk analysis model 27
3.4 A New Methodology for Security Evaluation in Cloud Computing 29
3.5 Using ISO 27001 in Teaching Information Security 30

4. Preguntas, objetivos y metodología de la investigación **33**
4.1 Preguntas de Investigación 33
4.2 Objetivo General 33
4.3 Objetivos específicos 33

5. Metodología propuesta **35**
5.1 Implementación del método Delphi 35
5.2 Prototipo para evaluación de controles 47
5.3 Caso de Estudio 56

6. Conclusiones y recomendaciones **70**
6.1 Conclusiones 70
6.2 Recomendaciones 72
6.3 Trabajo Futuro 72

Bibliografía **75**

Anexos **81**

Perfiles de los expertos que participaron **81**

Encuesta enviada a expertos **82**

Tabla de calificación y resultados **85**

Lista de figuras

Pág.

Figura 1-1: Modelo de Deming (Deming, 1989) 3
Figura 1-2: Modelo PHVA aplicado a los procesos de los SGSI (International Organization for Standardization, 2005b). 5
Figura 1-3: Secciones ISO/IEC 27001 (International Organization for Standardization, 2013a). 6
Figura 1-4: Fases para la implementación de un SGSI 9
Figura 1-5: Cantidad certificaciones ISO/IEC 27001 Colombia (International Organization for Standardization, 2015) 11
Figura 1-6: Cantidad certificaciones ISO/IEC 27001 Mundo (International Organization for Standardization, 2015) 12
Figura 1-7: Cantidad certificaciones ISO 9001 Mundo (International Organization for Standardization, 2015) 13
Figura 1-8: Integración de gente, procesos y tecnología ITIL (Acevedo, 2010) 15
Figura 1-9: Modelo de estrategia del servicio (De Sousa Pereira & Da Silva, 2010) 16
Figura 1-10: Principio funcionamiento COBIT (ISACA, 2007) 18
Figura 1-11: Características Gobierno de TI (ISACA, 2012) 18
Figura 3-1: Escala de tiempo de detecciones y acciones proactivas (Hajdarevic & Allen, 2013) 25
Figura 3-2: Cantidad de controles en comparación BS7799, 27001:2005 y 27001:2013 26
Figura 3-3: Modelo de clasificación de riesgos (Peciña et al., 2011) 29
Figura 3-4: Arquitectura empresarial para evaluación de seguridad (National Institute of Standards and Technology, 2011) 30
Figura 3-5: Modelo de procesos para implementación SGSI (Talib et al., 2012) 31
Figura 5-1: Bloque de preguntas para encuesta 1 (Elaboración propia) 37
Figura 5-2: Modelo de evaluación Delphi (Elaboración propia) 40
Figura 5-3: Proceso de comparación Alfa Cronbach (Elaboración propia) 44
Figura 5-4: Estructura del cuestionario de calificación de control (Elaboración propia) .. 45
Figura 5-5: Pantalla inicial (Elaboración propia) 48
Figura 5-6: Registro de experto (Elaboración propia) 49
Figura 5-7: Secciones de variables creadas (Elaboración propia) 50
Figura 5-8: Variable títulos profesionales (Elaboración propia) 51
Figura 5-9: Controles agregados para evaluación (Elaboración propia) 52
Figura 5-10: Preguntas registradas para evaluación (Elaboración propia) 53
Figura 5-11: Valoración y peso que se le dio al experto (Elaboración propia) 54

Figura 5-12: Calificación de preguntas asociadas a control (Elaboración propia).....55
Figura 5-13: Resultado de valoración de un control (Elaboración propia).....56

Lista de Tablas

Tabla 1-1: Procesos de un SGSI (International Organization for Standardization, 2013b).8
Tabla 1-2: Certificaciones ISO/IEC 27001 en 2015 (International Organization for Standardization, 2015) 10
Tabla 1-3: Ranking de países por cantidad de certificaciones ISO/IEC 27001 (International Organization for Standardization, 2015)..... 11
Tabla 1-4: Cantidad de certificaciones ISO/IEC 27001 en el tiempo a nivel mundial (International Organization for Standardization, 2015)..... 12
Tabla 1-5: Cantidad de certificaciones ISO 9001 en el tiempo a nivel mundial (International Organization for Standardization, 2015)..... 13
Tabla 3-1: Tabla de clasificación de riesgos (Peciña et al., 2011)..... 28
Tabla 5-1: Formato de encuesta enviado de método Delphi (Elaboración propia) 38
Tabla 5-2: Formato de método Delphi consolidado (Elaboración propia) 39
Tabla 5-3: Variable de calificación de perfil de experto (Elaboración propia) 40
Tabla 5-4: Escala Likert de variable años de experiencia (Elaboración propia)..... 41
Tabla 5-5: Escala Likert de variable nivel de formación (Elaboración propia)..... 41
Tabla 5-6: Escala Likert de variable sector económico (Elaboración propia)..... 41
Tabla 5-7: Escala Likert de variable título profesional (Elaboración propia)..... 42
Tabla 5-8: Escala Likert de variable certificación (Elaboración propia)..... 42
Tabla 5-9: Pesos y características de los expertos evaluadores (Elaboración propia) ... 42
Tabla 5-10: Escala de valoración Alfa de Cronbach (Frías Navarro, 2014)..... 43
Tabla 5-11: Calificación y resultado de control de SGSI (Elaboración propia)..... 46
Tabla 5-12: Clasificación de resultados CVSS (FIRST, 2015)..... 47
Tabla 5-13: Controles evaluados en compañía de financiamiento (Elaboración propia)(International Organization for Standardization, 2013b)..... 57
Tabla 5-14: Clasificación por cantidad de controles (Elaboración propia) 69

Lista de Símbolos y abreviaturas

Abreviaturas

Abreviatura	Término
SGSI	Sistema de gestión de seguridad de la información
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
PHVA	Planear, hacer, verificar y actuar
CVSS	Common Vulnerability Scoring System
ISMS	Information security management system
OCDE	Organización para la Cooperación y el Desarrollo Económicos
GPL	General public license
NTC	Norma técnica colombiana
BS	British Standards
PDP	Policy Decision Point
GQM	Goal, question, metric
ITIL	Information Technology Infrastructure Library
COBIT	Control Objectives for Information and related Technology
NIST	National Institute of Standards and Technology
ISACA	Information Systems Audit and Control Association

Introducción

El estándar ISO/IEC 27001 se desarrolló con el objetivo de proporcionar los requisitos que permiten “establecer, implementar, mantener y continuamente mejorar un sistema de gestión de seguridad de la información”. El estándar ISO/IEC 27001 se puede implementar para evaluar la habilidad que tienen las organizaciones para cumplir sus propios requisitos de seguridad de la información (Pavlov & Karakaneva, 2011).

Los requisitos propuestos por esta norma son aplicables a todo tipo de organización. El modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA) es implementado en el estándar ISO/IEC 27001 con el objetivo de estructurar los procesos de los SGSI (sistemas de gestión de seguridad de la información) que utilizan las organizaciones (García, Quispe, & Ráez, 2003).

Los SGSI tienen por objetivo brindar conocimiento acerca del tratamiento adecuado de la información y de todo activo digital que pueda representar un riesgo en las manos equivocadas (Susanto, Almunawar, & Tuan, 2011). Los procesos de gestión de riesgos que se implementan en los SGSI ayudan a preservar la confidencialidad, la integridad y disponibilidad de la información (Broderick, 2006). El estándar ISO/IEC 27001 define un SGSI como “parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información” (International Organization for Standardization, 2013b)

Dentro de las organizaciones es clave mantener la información asegurada, sin embargo, muchas compañías no son conscientes de los riesgos que corren al no tener controles de seguridad, para minimizar esos riesgos existen los llamados SGSI, los cuales contienen una serie de controles que permitirán verificar con el tiempo el nivel de seguridad de la información; la frecuente ocurrencia de eventos de riesgo operacional genera pérdidas económicas y deterioro de la imagen en diferentes organizaciones, lo cual invita a la evaluación de la efectividad de las actividades de control que se realizan en el manejo de seguridad de la información (Beckers, Hofbauer, Quirchmayr, & Wills, 2013), el caso

Manning, que filtró miles de documentos del ejército de Estados Unidos, o el caso Snowden que divulgó información clasificada de la NSA, son evidencia del reto que supone la implementación adecuada de un SGSI, y la correcta elección de controles para tener un nivel de efectividad que permite mitigar los riesgos más altos o críticos (Cleave, 2013).

En este trabajo se propone una metodología, que permite identificar los controles clave, a partir del relacionamiento de variables cualitativas definidas y valoradas por expertos en temas de auditoría del estándar ISO/IEC 27001. Se realizó el estudio de un caso real, en una compañía de financiamiento, se implementó un SGSI basado en el estándar ISO/IEC 27001, los diferentes objetivos de control fueron seleccionados usando el método Delphi, con una base de conocimiento de 7 expertos, el tiempo de implementación fue de doce meses.

La estructura del presente trabajo es la siguiente. En el capítulo 1 se presenta el marco teórico, el cual incluye una descripción del estándar ISO 27001 para la gestión de la seguridad de la información y de los SGSI, además de ITIL y COBIT, los cuales son usados frecuentemente como alternativas uno del otro. En el capítulo 2 se presenta el problema. En el capítulo 3 se presenta la revisión de la literatura de los casos estudiados como modelos propuestos en los SGSI. En el capítulo 4 se presentan los objetivos. En el capítulo 5 se presenta la metodología de evaluación y el prototipo desarrollado y en el capítulo 6 se presentan las conclusiones.

1. Marco Teórico

En este capítulo se presentan las definiciones, fundamentos de teoría y los conceptos de los elementos fundamentales en los cuales está basada esta investigación.

1.1 Modelo de Deming

El estándar ISO/IEC 27001 tiene como enfoque la seguridad de la información, y se desarrolló con el objetivo de proporcionar los requisitos que permiten “establecer, implementar, mantener y continuamente mejorar un sistema de gestión de seguridad de la información” (International Organization for Standardization, 2013b), basado en el modelo de Deming, el cual se puede observar en la Figura 1-1.

Figura 1-1: Modelo de Deming (Deming, 1989)

Edwards Deming, un profesor de la Universidad de Columbia, Estados Unidos, fue precursor de un modelo organizacional basado en dos premisas fundamentales, las cuales era:

1. Promover y fortalecer la cooperación y ayuda entre todos los ámbitos de una organización, tanto internos como externo (W. Edwards Deming, 1989).
2. Promover y fortalecer el continuo aprendizaje que permita facilitar las mejores prácticas en pro de toda la gestión de procesos (W. Edwards Deming, 1989).

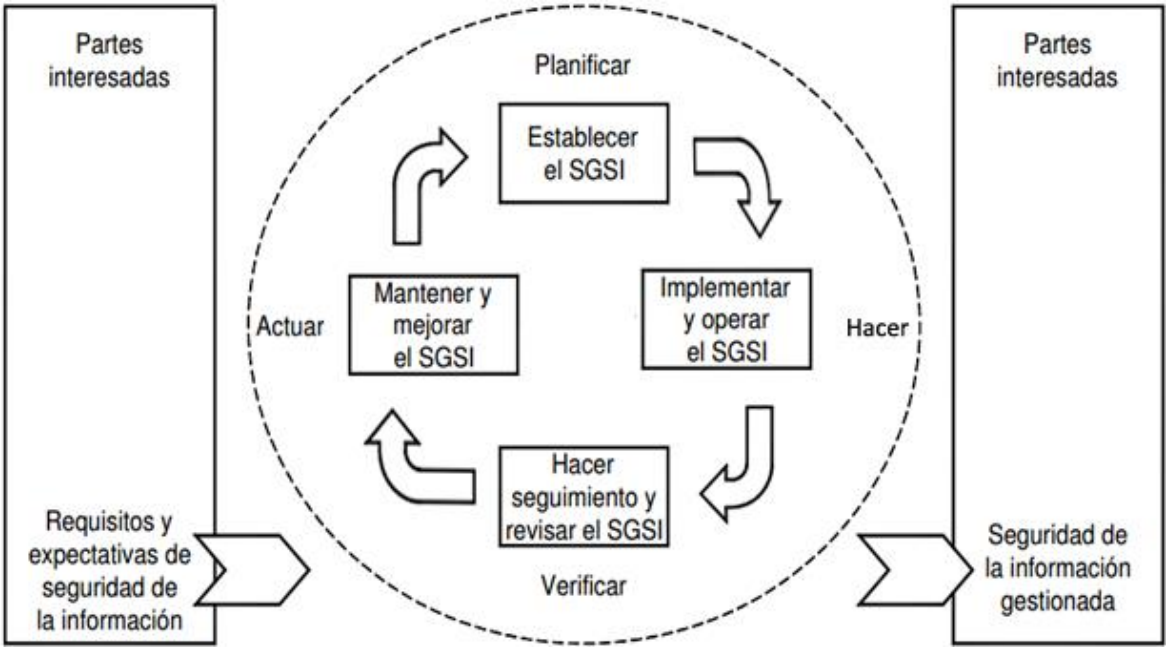
Deming proponía satisfacción de los trabajadores, mejora continua de los procesos, los productos y los servicios para garantizar la supervivencia y además la evolución organizacional.

El modelo de Deming aplicado a los SGSI se puede observar en la Figura 1-2. “La adopción del modelo PHVA refleja los principios establecidos en las directrices OCDE (Organización para la Cooperación y el Desarrollo Económico) que controlan la seguridad de sistemas y redes de información” (OCDE, 2002). En la primera fase de este ciclo, la cual es *planificar*, se deben entregar resultados alineados con las políticas y objetivos de una organización, para ello se deben establecer políticas, objetivos, procesos y procedimientos de seguridad. En la segunda fase, *hacer*, se deben implementar y operar todos los controles que se hayan propuesto en el SGSI al igual que las políticas y los procesos. En la tercera fase, *verificar*, se debe realizar un reporte de los resultados con base en la evaluación y medida del desempeño del proceso del SGSI de acuerdo a las políticas y objetivos de seguridad planteados. En la cuarta y última fase del modelo PHVA, la cual es *actuar*, se deben “emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI”, para lograr una mejora continua del SGSI (W. Edwards Deming, 1989)(Susanto et al., 2011).

Además, Deming propone un modelo gerencial de gestión total de la calidad basado en 14 principios fundamentales, los cuales son (W. Edwards Deming, 1989):

1. Creación y comunicación de la visión, el propósito y la misión de la organización.
2. Aprendizaje y adopción de la filosofía gerencial.
3. Evitar el someter a los sujetos a la inspección masiva como medio de motivación para la productividad.
4. El precio no será el único factor que se considere para realizar una compra.
5. Perfeccionar mediante la mejora continua de la calidad, los sistemas de producción y de servicio.
6. Establecer la capacitación en el trabajo.
7. Promover, enseñar e instituir el liderazgo.
8. Combatir el temor propiciando un clima organizacional que favorezca la motivación.
9. Derribar las barreras que existen entre las diferentes áreas de la organización.
10. Eliminar los lemas, exhortaciones y metas meramente numéricas para los trabajadores.
11. Eliminar los estándares de producción y las cuotas numéricas, sustituyéndolos por el mejoramiento continuo de la calidad.
12. Eliminar los obstáculos que conspiren contra el orgullo de los trabajadores por el haber realizado un buen trabajo.
13. Instituir programas robustos de educación y reentrenamiento.
14. Emprender acciones para alcanzar la transformación organizacional.

Figura 1-2: Modelo PHVA aplicado a los procesos de los SGSI (International Organization for Standardization, 2005b).



1.2 SGSI – Sistema de gestión de seguridad de la información

El estándar ISO/IEC 27001 proviene de una familia de normas llamada ISO/IEC 27000, la cual tiene la intención de ayudar a las organizaciones de todo tipo y tamaño a implementar y operar un SGSI, y consta de varias normas internacionales bajo el título de *tecnologías de la información – técnicas de seguridad* (International Organization for Standardization, 2005a).

El estándar ISO/IEC 27001 se encuentra dividido en 10 secciones, como se puede ver en la Figura 1-3.

Figura 1-3: Secciones ISO/IEC 27001 (International Organization for Standardization, 2013a).

Esta familia de la ISO/IEC promueve la adopción del enfoque basado en procesos, para que una organización funcione efizcamente, se deben identificar y gestionar muchas actividades, por lo que se considera como proceso a cualquier actividad que consume recursos y que además su gestión promueva la transformación de ingresos en salidas. A menudo, el resultado de un proceso constituye el ingreso para un proceso siguiente (Fung, Farn, & Lin, 2003).

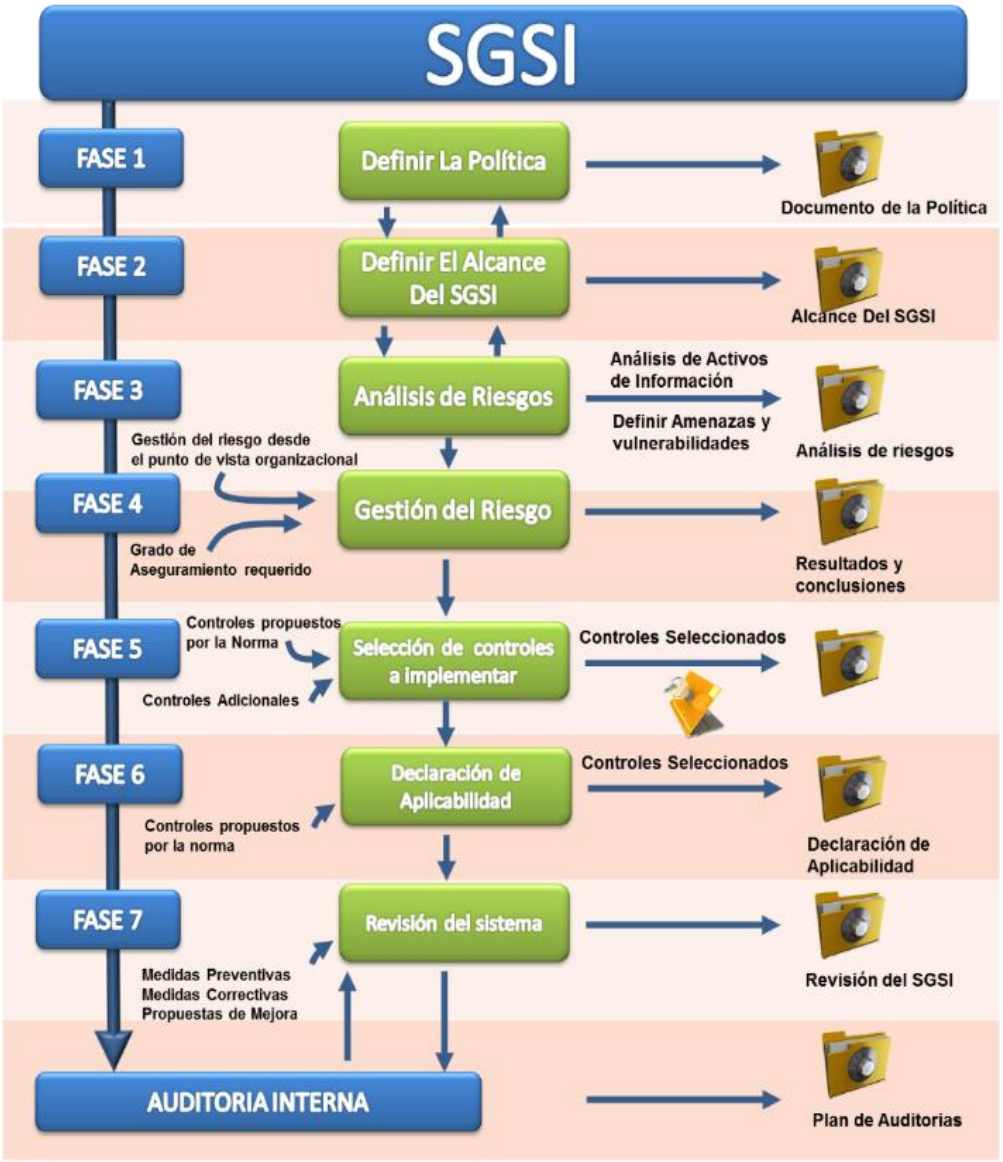
El enfoque basado en procesos consiste en que la organización identifique las actividades del funcionamiento de esta y la interacción entre las actividades, así para la gestión de la seguridad de la información se hace énfasis en la importancia de (International Organization for Standardization, 2013b): ver Tabla 1-1

Tabla 1-1: Procesos de un SGSI (International Organization for Standardization, 2013b).

Etapa	**Descripción**
Planificar (Establecer el SGSI)	Establecer la políticas, objetivos, procesos y procedimientos del SGSI pertinentes a la gestión del riesgo y mejorar la seguridad de la información para obtener resultados de acuerdo con las políticas y objetivos generales de la organización.
Implementar (Implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos del SGSI.
Medir (Monitorear y revisar el SGSI)	Evaluar, y donde sea aplicable, medir el rendimiento del proceso contra la política del SGSI, sus objetivos y experiencia práctica, e informar los resultados para gestionar su revisión.
Mejorar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de auditorías internas del SGSI y de revisión de gestión u otra información relevante, para lograr mejora continua del SGSI.

El estándar ISO/IEC 27001 define siete fases para la implementación de un SGSI bajo sus controles, los cuales se pueden observar en la Figura 1.4.

Figura 1-4: Fases para la implementación de un SGSI (“Iso 27001,” n.d.)



El estándar ISO/IEC 27001 establece un nivel de gobierno TI , pues es necesaria la administración, comprensión y el uso de las TI como un facilitador para alcanzar los objetivos del negocio de manera eficaz, para lograr esto se requiere conocer los riesgos actuales, emergentes, y el impacto posible, ya que la norma debe evitar los peores riesgos

relacionados con TI (Susanto, Almunawar, & Tuan, 2012)(Neubauer, Ekelhart, & Fenz, 2008). La implementación de los SGSI en las organizaciones está basada en "las necesidades, objetivos, procesos, tamaño, estructura y requerimientos de seguridad únicos" (Shojaie, Federrath, & Saberi, 2014). Los SGSI son una parte importante de las organizaciones, ya que estos proveen un conjunto de políticas procedimientos, directrices, recursos y actividades que deben ser gestionadas (Shojaie et al., 2014).

La seguridad de la información está definida por tres características principales, las cuales son (Nancylia, Mudjtabar, Sutikno, & Rosmansyah, 2014):

- **Confidencialidad**: Este atributo indica que la información debe ser visible únicamente para las personas autorizadas.

- **Integridad**: Este atributo vela porque la exactitud de la información, la validez y la completitud se mantengan en todo momento, protegiéndola de alteraciones o modificaciones que no estén autorizadas.

- **Disponibilidad**: Este atributo garantiza el acceso a la información en todo momento que se requiere, siempre y cuando este acceso esté autorizado.

EL estándar ISO/IEC 27001 se consolida a nivel mundial como un referente de calidad y como la oportunidad que ven muchas organizaciones para certificar sus procesos con intenciones de mejora reputacional, productividad y formación integral. Sin embargo, a pesar de que la seguridad de la información es un tema que le compete a cualquier organización independientemente de su enfoque de negocios o área de productividad, es más común que los SGSI sean implementados por organizaciones que están relacionadas con las tecnologías de la información (ISACA, 2012)(García et al., 2003), como puede verse en la Tabla 1-2 , en la cual se refleja la cantidad de certificaciones ISO/IEC 27001 otorgadas por la ISO de acuerdo al sector industrial de quien realiza la solicitud.

Tabla 1-2: Certificaciones ISO/IEC 27001 en 2015 (International Organization for Standardization, 2015)

Top five industrial sectors for ISO/IEC 27001 certificates 2015

1	Information technology	5573
2	Other Services	959
3	Transport, storage and communication	301
4	Electrical and optical equipment	296
5	Health and social wprl	231

En Colombia, el panorama es desalentador en comparación con las grandes economías mundiales, de todos modos, los indicadores van creciendo día a día y para el 2015 se realizaron 184 certificaciones de ISO/IEC 27001, comparado con las 8240 certificaciones obtenidas en Japón, ver Figura 1-5 con el indicador en el tiempo para Colombia y Tabla 1-3 con el top de los países en certificación a nivel mundial.

Figura 1-5: Cantidad certificaciones ISO/IEC 27001 Colombia (International Organization for Standardization, 2015)

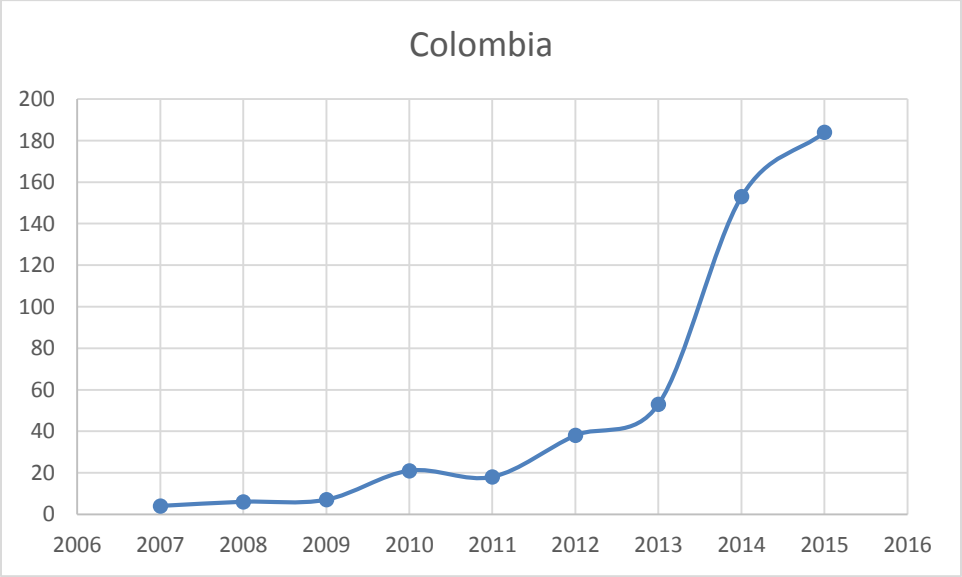


Tabla 1-3: Ranking de países por cantidad de certificaciones ISO/IEC 27001 (International Organization for Standardization, 2015)

Top 10 countries for ISO/IEC 27001 certificates - 2015

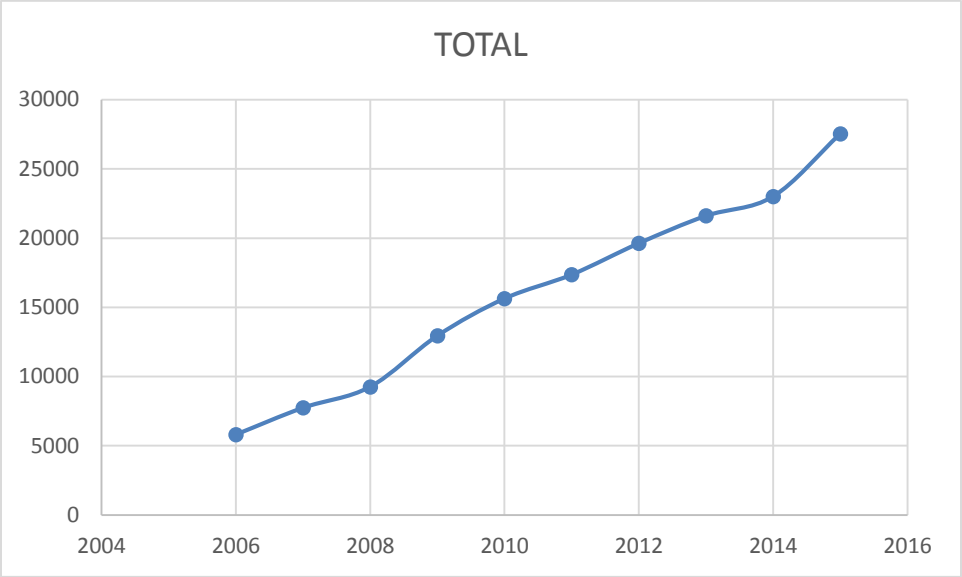
1	Japan	8240
2	United Kingdom	2790
3	India	2490
4	China	2469
5	United States of America	1247
6	Romania	1078
7	Italy	1013
8	Germany	994
9	Taipei, Chinese	939
10	Spain	676

A nivel mundial, las certificaciones ISO/IEC 27001 van en aumento cada año, como puede verse en la Tabla 1-4 y Figura 1-6, en donde en nueve años, casi se ha quintuplicado el número de organizaciones certificadas en el estándar.

Tabla 1-4: Cantidad de certificaciones ISO/IEC 27001 en el tiempo a nivel mundial (International Organization for Standardization, 2015)

Año	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
TOTAL	5797	7732	9246	12935	15626	17355	19620	21604	23005	27536

Figura 1-6: Cantidad certificaciones ISO/IEC 27001 Mundo (International Organization for Standardization, 2015)

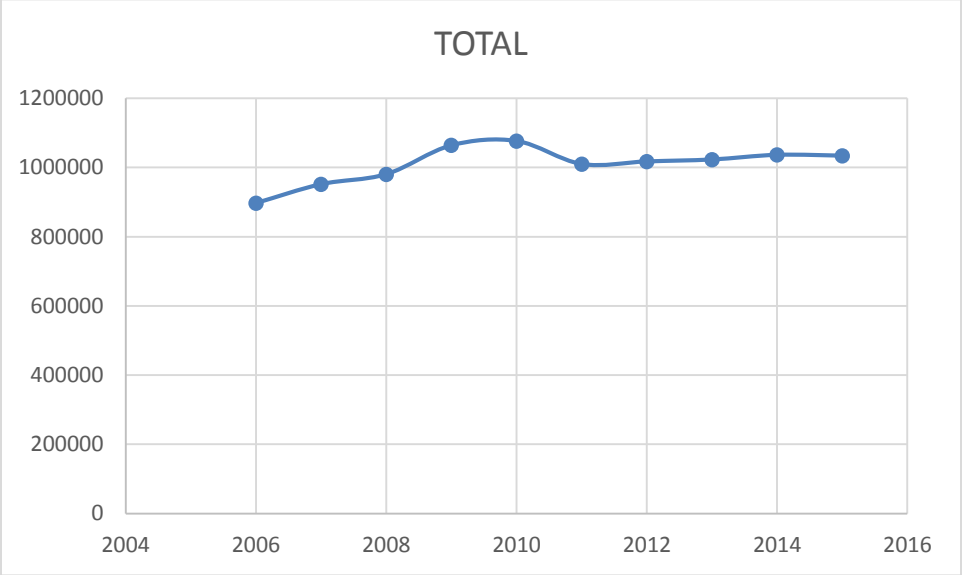


Realizando una comparación de la magnitud de las certificaciones ISO, vemos en la Tabla 1-5 y Figura 1-7, que el estándar ISO 9001 es certificado 38 veces más que el estándar ISO/IEC 27001.

Tabla 1-5: Cantidad de certificaciones ISO 9001 en el tiempo a nivel mundial (International Organization for Standardization, 2015)

Año	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
TOTAL	896905	951486	980322	1063751	1076525	1009845	1017279	1022877	1036321	1033936

Figura 1-7: Cantidad certificaciones ISO 9001 Mundo (International Organization for Standardization, 2015)



1.3 ITIL- Information Technology Infrastructure Library

ITIL es un marco de referencia que describe una serie de mejores prácticas y métodos para la administración de servicios de tecnologías de la información, enfocado principalmente en la administración de procesos conocida como gobernanza IT(Arraj, 2013). La idea de ITIL es crear una relación entre los procesos, la tecnología y los recursos humanos (Iden & Eikebrokk, 2013), ver Figura 1-8.

Figura 1-8: Integración de gente, procesos y tecnología ITIL (Acevedo, 2010)

ITIL contiene información sobre las metas propuestas en mejoras de servicios, actividades generales, las diferentes entradas y salidas que se pueden incorporar a las áreas de IT(Tan, Cater-Steel, & Toleman, 2009). Actualmente Itil se publica en una serie de cinco libros, los cuales están estructurados de la siguiente manera:

- **Estrategia del servicio**: Sugiere considerar la gestión de servicios como un activo estratégico.

- **Diseño del servicio**: Sugiere transformar los objetivos estratégicos en portafolios y activos.

- **Transición del servicio**: Cubre el proceso de toda la transición a nuevos servicios y mejoras.

- **Operación del servicio:** Cubre las mejores prácticas para gestionar la operación del servicio diario.

- **Mejora continua del servicio**: Proporciona un método de mantenimiento ofrecido a los clientes para el diseño del servicio, transición del servicio y operación del servicio.

ITIL es mantenido por Axelos, compañía británica que se encarga de actualizar el marco de referencia y publicar las mejoras del gobierno IT ITIL.

Así mismo, Axelos es encargada de certificar el conocimiento de las personas, las cuales pueden recibir un aval sobre sus conocimientos de parte de las entidades certificadoras autorizadas por Axelos. Las empresas no se pueden certificar oficialmente en ITIL, sin embargo, pueden ser auditadas por empresas externas obteniendo un diagnóstico en el cual se pueda decir que está alineada con ITIL.

El gobierno de TI surge por la necesidad de alinear TI con el negocio, demostrar una sincronía entre las metas de la organización y el correcto funcionamiento de TI que ayuda a conseguir esas metas, para lo cual se requiere (ISACA, 2012):

- Lograr una relación valor/costo.
- Mantener la seguridad de la información.
- Mantener la operación de TI.
- Administrar la complejidad.
- Cumplir con los requerimientos regulatorios y contractuales.

ITIL basa de funcionamiento en una estrategia de servicios orientados al cliente, que puede resumirse en la Figura 1-9 (De Sousa Pereira & Da Silva, 2010).

Figura 1-9: Modelo de estrategia del servicio (De Sousa Pereira & Da Silva, 2010)

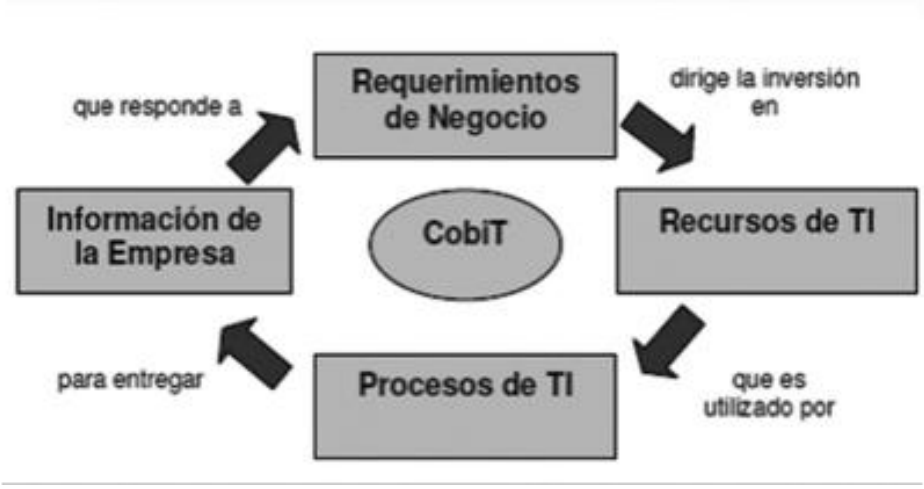
- La estrategia de servicio proporciona orientación como como diseñar, desarrollar e implementar la administración de servicios.
- Servicio del diseño proporciona orientación para el desarrollo de servicios y procesos de gestión de servicios, comprende los métodos para convertir objetivos en carteras de servicios y activos de servicios.
- Servicio de transición proporcionan desarrollo y mejora de las capacidades de transición para las nuevas o mejoradas operaciones.
- Servicio de operación proporciona orientación para la eficacia y eficiencia en la prestación y apoyo de servicios para garantizar el valor para el cliente.
- Mejora continua del servicio proporciona una guía instrumental para crear y mantener el valor para los clientes a través de un mejor servicio.

1.4 COBIT – Control Objectives for Information and Related Technology

COBIT es un marco de referencia con objetivos detallados y prácticas de control orientado al negocio, no se enfoca únicamente en el gobierno IT, pues cubre todas las funciones y procesos dentro de cualquier organización y sirve como guía integral para los dueños de los

procesos y gerencias, tiene como propósito satisfacer la necesidad de disponer información de calidad para el soporte de las decisiones del negocio como se ve en Figura 1-10 (ISACA, 2012).

Figura 1-10: Principio funcionamiento COBIT (ISACA, 2007)



COBIT, como gobierno de TI y marco de referencia tiene enfoque en dos áreas muy importantes (Blanco, Lasheras, Fernández-Medina, Valencia-García, & Toval, 2011) :

- El tratamiento de la información como el uso combinado de los procesos de TI y los recursos de TI.

- Brindar la información que se requiere para el apoyo de los diferentes requerimientos en el tiempo del negocio y los objetivos de la organización.

COBIT define las siguientes áreas como principales para el gobierno de TI Figura 1-11

Figura 1-11: Características Gobierno de TI (ISACA, 2012)

Alineación Estratégica

Está enfocada en asegurar la conexión entre los planes de TI y los planes de la organización para el negocio (Paola & Cadavid, 2011).

Entrega de valor

Está relacionada con la ejecución de los planes de TI, salvaguardando el enfoque que siempre debe estar alineado con la optimización de costos y máximo beneficio de productividad (Paola & Cadavid, 2011)..

Administración de los recursos

Propicia el uso adecuado de los recursos, tanto tangibles como intangibles, como lo son el personal, los equipos de infraestructura y la base de conocimientos del negocio (Paola & Cadavid, 2011)..

Administración del riesgo

Propende por delegar las responsabilidades de administración del riesgo en la organización, dando por aceptado el entendimiento del compromiso de cada área en dar su aporte para la no materialización de los riesgos que debe mitigar el sistema de gestión (Paola & Cadavid, 2011)..

Medición del desempeño

Realiza un seguimiento y monitoreo de todo el plan de TI de acuerdo a los proyectos, servicios y procesos que competen para estar alineados con los objetivos del negocio (Paola & Cadavid, 2011)..

COBIT se encuentra en la versión 5, es mantenido por ISACA – Information Systems Audit and Control Association, cuenta con tres certificaciones personales brindadas al personal en general, las cuales son (ISACA, 2016):

- COBIT 5 – Fundamentos: Certifica el conocimiento y comprensión del gobierno TI y gestión de las tecnologías de la información proporcionadas por COBIT.

- COBIT 5 – Implementación: Certifica el conocimiento para implementar conjunto de procedimientos y buenas prácticas de COBIT.

- COBIT 5 – Evaluador: Esta certificación sirve para sugerir las mejoras del proceso, para entregar valor al negocio, para medir el logro de los objetivos de negocio actuales o en proyecto.

COBIT tiene siete categorías de acción, de ellas, tres ya se mencionan en la ISO/IEC 27001 que son: Confidencialidad, Integridad, Disponibilidad. Las otras cuatro categorías que contempla COBIT son (ISACA, 2007):

- **Efectividad:** Indica que la información debe ser pertinente para la actividad o proceso de negocio en la que se encuentra, así mismo que sea entregada oportunamente y de manera utilizable.

- **Eficiencia:** Se refiere a la entrega de información de la manera más económica y productiva.

- **Cumplimiento:** Indica que el proceso o actividad debe estar alineado con las regulaciones o leyes actuales del negocio.

- **Confiabilidad de la información:** Está relacionado con que en los procesos la información utilizada sea la apropiada y la que realmente se requiere.

2. Problema y justificación de la investigación

El proceso de implementar un SGSI es considerado como un desafío en las organizaciones hoy en día, las organizaciones consideran la implementación de nuevos procesos relacionados con la seguridad como uso de tiempo en actividades no productivas (Boehmer, 2009).

Los implementadores que inician el proceso en una organización, tienen muchas dificultades para establecer las métricas con las cuales se evaluarán los controles establecidos en el SGSI, ya que los procesos en cada organización están adaptados a cada necesidad (Hajdarevic & Allen, 2013).

Dentro de los principales problemas con los que se encuentran al momento de implementar un SGSI se destacan (Vanaclocha, 2009):

- Esta implementación sólo le corresponde al área de TI.
- Después de implementado no será necesario volver a saber del SGSI en mucho tiempo.
- Las personas no han identificado claramente cuáles son los riesgos asociados a los procesos en los que se encuentran involucrados.

Pero un problema muy grave que se ha detectado en la selección de controles de un sistema de gestión a nivel general es que la selección y evaluación de los controles a implementar, con el fin de que tengan más efectividad o se implementen en menor tiempo, son seleccionados por procedimientos que se basan en la percepción y experiencia de los expertos que implementan el SGSI, (Pierce & Sweeney, 2005) destacan la presencia de acciones y procedimientos de control que no están formalizados en los implementadores y que pueden resultar siendo desfavorables para la relación costo/beneficio de la implementación del SGSI.

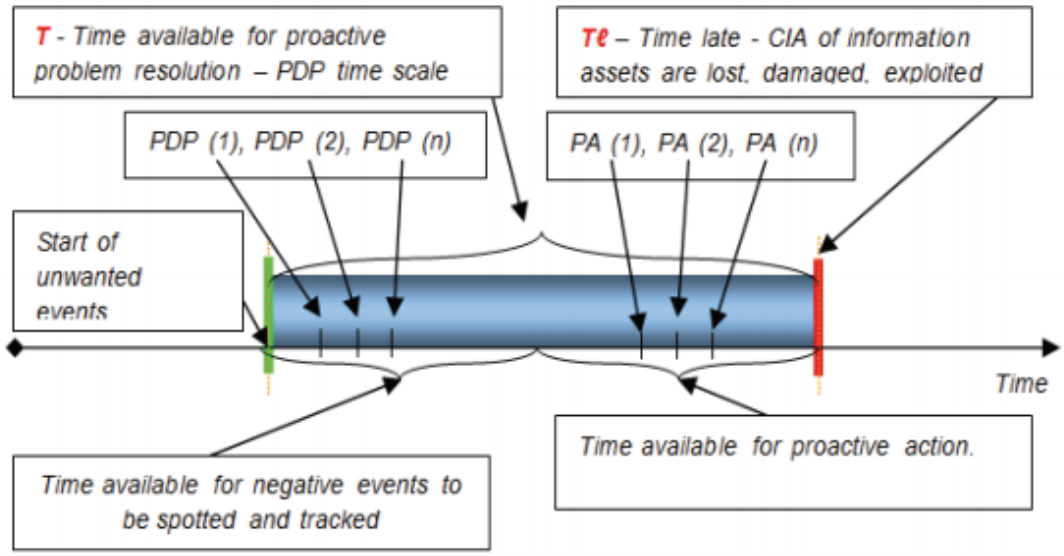
Considerando esta problemática, se encuentra la necesidad de proponer y desarrollar una nueva metodología que le permite a un implementador de un SGSI obtener una medición consolidada de los controles del estándar ISO/IEC 27001, en la que a partir de una valoración estadística se pueda contar con un apoyo técnico para seleccionar los controles más efectivos para la organización.

3. Revisión de literatura

3.1 A New Method for the Identification of Proactive Information Security Management System Metrics

(Hajdarevic & Allen, 2013) proponen un nuevo método de planificación proactiva basado en el modelo GQM (Goal, Question, Metric) (Meta-Pregunta-Métrica), en el cual los riesgos detectados en un análisis se convierten en objetivos mayores y se dividen en objetivos menores, a cada uno de esos pequeños objetivos se le asignan métricas para determinar si son resueltos, consideran que existe una ventana de tiempo antes que un riesgo se materialice, y es en ese momento previo en el que resolviendo los pequeños objetivos correspondientes se puede mitigar el riesgo, todo esto desde el punto de vista 'divide y vencerás'. Se presenta en la Figura 3-1 una escala de tiempo en la cual hay varios puntos de control llamados PDP, un límite de tiempo en el cual se puede hacer una identificación proactiva de los controles que están siendo efectivos antes de que se vea comprometido el objetivo mayor.

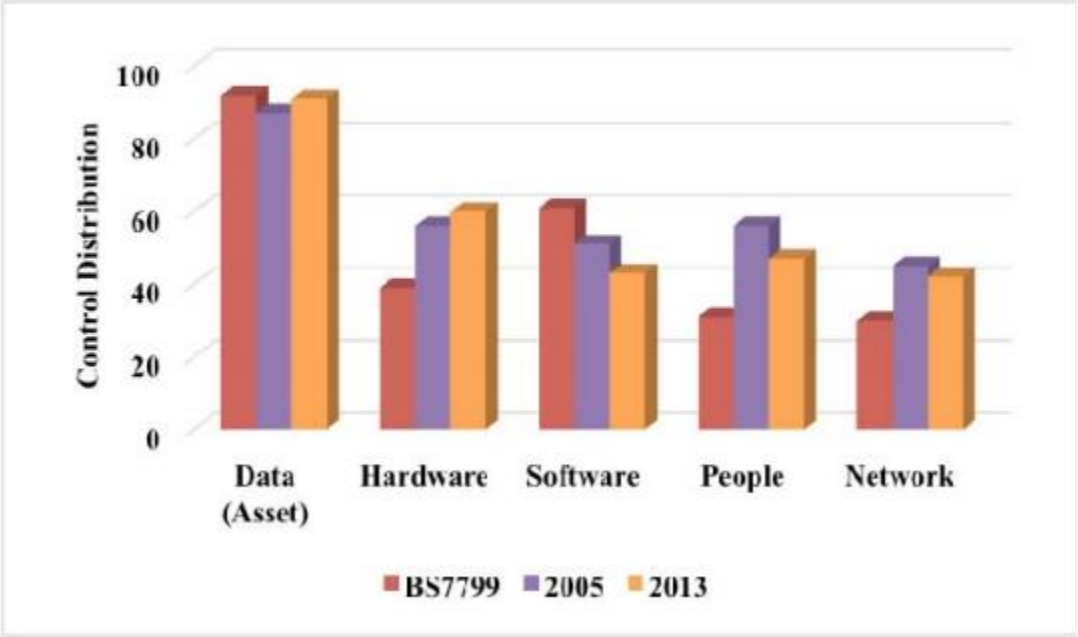
Figura 3-1: Escala de tiempo de detecciones y acciones proactivas (Hajdarevic & Allen, 2013)



3.2 Evaluating the effectiveness of ISO 27001:2013 based on Annex A

(Shojaie et al., 2014) realizan una comparación entre el estándar ISO/IEC 27001:2005 e ISO/IEC 27001:2013. Los autores clasifican los controles de estos estándares en 5 categorías: data, hardware, software, people y network. Estas categorías permiten de manera más fácil que pequeñas y medianas empresas implementen los controles necesarios y relevantes basándose en sus propias necesidades, de acuerdo a la evolución del estándar ISO/IEC 27001, se plantea que el foco de la implementación de controles debe estar en los que protegen directamente los datos y posteriormente en el hardware que almacena dichos datos. La categoría de software se encuentra en tercer lugar disminuyendo cada vez la cantidad de controles que la protegen, debido al aumento de la contratación o compra de licencias de software frente al desarrollo en casa, los controles de usuarios y de la infraestructura han aumentado y no pueden perder importancia, ya que son la primera barrera externa de la información, es lo que plantean los autores, ver Figura 3-2.

Figura 3-2: Cantidad de controles en comparación BS7799, 27001:2005 y 27001:2013



Comparación entre BS7799, ISO27001:2005, ISO27001:2013, en las categorías propuestas.

3.3 Physical and logical security risk analysis model

(Peciña, Bilbao, & Bilbao, 2011) proponen una metodología para el análisis de riesgos de los procesos de activos físicos y activos de información, es una metodología dirigida a organismos de administración y a organismos empresariales principalmente. La metodología se basa en el estándar ISO/IEC 27001 y ISO/IEC 31000. Resulta confusa la propuesta de los autores, ya que se refieren a ésta como una *metodología*, como un *método* y también como un *modelo*. La metodología propuesta contiene indicadores y criterios que se pueden implementar para evaluar y comparar tanto los riesgos físicos como los riesgos de información, en ella se establecen los siguientes pasos para realizar el análisis de los controles:

A. Establecimiento del contexto: en este paso se identifican los activos, amenazas y tiempos.

B. Identificación de riesgos: en este paso se realiza una combinación de activos-amenazas-tiempos lo que constituye un riesgo

C. Análisis de riesgos: en este paso se estiman parámetros de riesgo que caracterizan a cada situación de riesgo y que se utilizarán para calcular el nivel de riesgo de acuerdo a una escala de valoración propia. Los cuatro parámetros a estimar son: impacto, criticidad, sensibilidad, necesidad de aseguramiento, la escala con la que miden es la que se muestra en la Tabla 3-1.

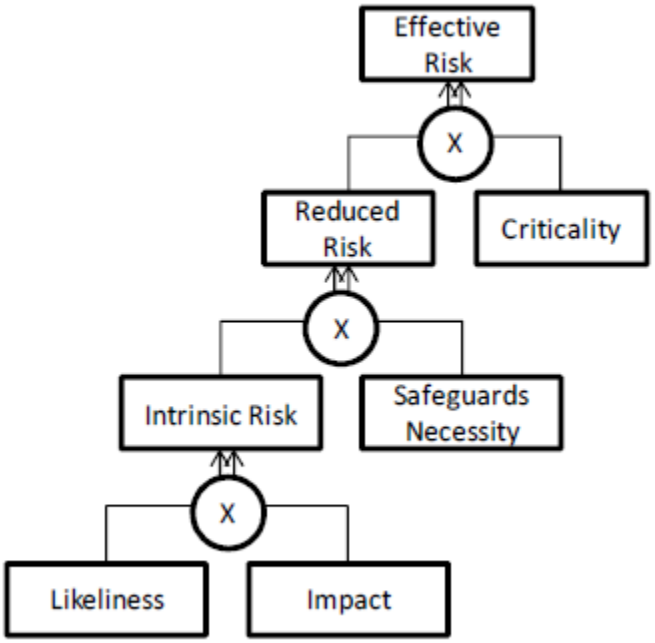
Tabla 3-1: Tabla de clasificación de riesgos (Peciña et al., 2011)

VH	Very High/Severe Impact for the Organization
H	High/Major Impact for the Organization
M	Moderate Impact for the Organization
L	Low/Minor Impact for the Organization
VL	Very Low/Negligible Impact for the Organization

D. Evaluación del riesgo: en este paso se realiza un cálculo de acuerdo a la escala obtenida anteriormente y clasifica el riesgo en un nivel, ver Figura 3-3, de acuerdo a la siguiente clasificación:

- Riesgo intrínseco: indica el daño probable producido por una amenaza a un activo en un momento dado, considerando que no hay controles que protejan el activo.
- Riesgo reducido: indica el daño probable producido por una amenaza a un activo en un momento determinado, considerando que los controles existentes que protegen el activo.
- Riesgo efectivo: indica el daño probable producido por una amenaza a un activo en un momento dado, considerando los controles existentes que protegen el activo y la criticidad que afecta al activo.

Figura 3-3: Modelo de clasificación de riesgos (Peciña et al., 2011)

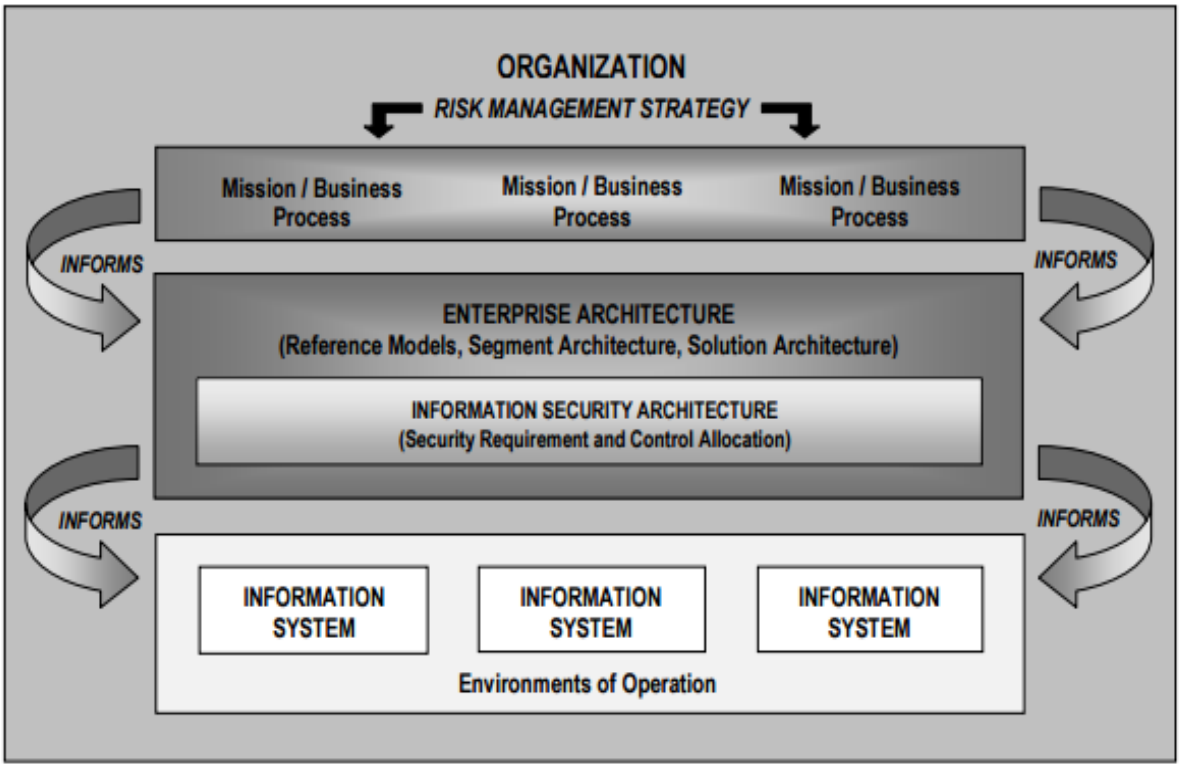


3.4 A New Methodology for Security Evaluation in Cloud Computing

(Ristov & Kostoska, 2012) proponen una extensión del estándar ISO/IEC 27001:2005 y también un nuevo control de virtualización dirigido a los sistemas en la nube. Los autores también proponen una métrica. Los autores consideran que tener el certificado del estándar ISO/IEC 27001 no es suficiente para sistemas de seguridad de la información, especialmente para la computación en la nube, por lo que se propone una adaptación de estándar ISO/IEC 27001 con la publicación 800-39 del Instituto Nacional de Estándares y Tecnología (NIST), entidad que brinda las directrices para seleccionar los controles de los sistemas de información en las organizaciones federales de Estados Unidos.

La metodología propuesta, integra los requisitos de seguridad en la arquitectura empresarial y los controles del estándar ISO/IEC 27001 como se puede ver en la Figura 3-4.

Figura 3-4: Arquitectura empresarial para evaluación de seguridad (National Institute of Standards and Technology, 2011)



3.5 Using ISO 27001 in Teaching Information Security

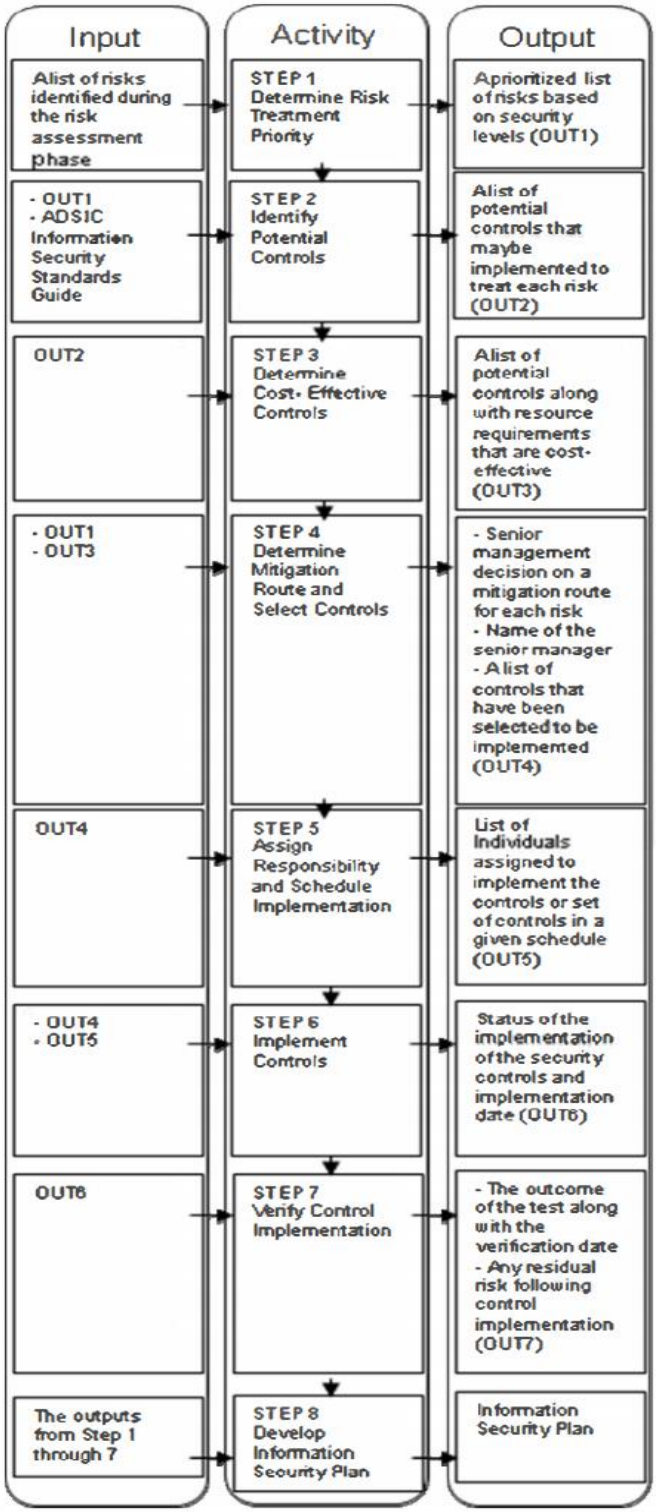
(Talib, Khelifi, & Ugurlu, 2012) muestran el proceso de la implementación de los SGSI que realizan en Abu Dhabi, Abu Dhabi Systems & Information Centre, este trabajo es importante porque se divide en tres partes la planeación de la implementación de un SGSI, dichas partes son:

- entradas
- actividades
- salidas

En la Figura 3-5 se observa un esquema de trabajo en el que los resultados de una actividad, son el insumo para el comienzo de otra, por lo que la selección de un control dependerá del anterior, y esto trae consigo el principal problema del modelo, y es que, si

se realiza una mala elección de controles, se puede caer en un error global, al ser dependientes unos de los otros.

Figura 3-5: Modelo de procesos para implementación SGSI (Talib et al., 2012)



4. Preguntas, objetivos y metodología de la investigación

4.1 Preguntas de Investigación

¿Cuáles factores dificultan el proceso de implementación del SGSI en las organizaciones?

¿Cómo se podría definir una metodología que contemple el concepto de muchos auditores y no sólo uno?

¿Cómo se podría definir una metodología que involucre las mejores prácticas de los diferentes marcos de referencia?

4.2 Objetivo General

Desarrollar una metodología para la evaluación del desempeño de los sistemas de gestión de seguridad de la información basado en la norma ISO/IEC 27001

4.3 Objetivos específicos

1. Proponer un modelo de evaluación objetiva por medio del método Delphi para controles de sistemas de gestión de seguridad de la información.
2. Contribuir con la identificación los controles claves que deben ser implementados en una organización para el sistema de gestión de seguridad de la información.

3. Implementar un prototipo de software basado en la metodología propuesta

5. Metodología propuesta

El estándar ISO/IEC 27001 proporciona orientación sobre la elaboración y uso de medidas para evaluar la eficacia de un SGSI, siendo estas aplicadas a la medición de controles o grupos de controles, sin embargo, no describen ni especifican cómo medir u evaluar la efectividad de los controles, ya que sólo se limitan a exigir su evaluación y cumplimiento (Pierce & Sweeney, 2005).

Dentro de las siete fases de implementación de un SGSI, este trabajo se concentra en la fase 5 y 6, que son: elección de controles a implementar y declaración de aplicabilidad, por lo que previamente, el implementador o el área de riesgo debió realizar la identificación de los riesgos y seleccionar cuáles de esos riesgos serán sujetos de implementación de controles de seguridad de la información.

Para establecer y determinar el peso de variables que conforman uno de los modelos que hacen parte del trabajo, se utilizó el método de expertos (Villagrasa, 2015), en el cual se realiza una consulta de opinión a diferentes personas que son expertos en el tema y tienen un criterio alto sobre el estándar ISO/IEC 27001, dichas variables serán tratadas más adelante.

Para extraer y maximizar las ventajas del método basado en expertos, se usa el método Delphi, ya que su metodología aprovecha la sinergia del grupo de expertos para eliminar las posibles interacciones no deseadas que pueden presentarse en el equipo con el fin de llegar a un consenso confiable (Almenara & Moro, 2014).

5.1 Implementación del método Delphi

Anonimidad: Durante el uso del método Delphi, los expertos no se conocen entre sí, esta condición tiene unos aspectos positivos, como son:

- Bloquea la posibilidad a los miembros de influenciar o ser influenciados por otros en su concepto.
- Permite que un experto pueda cambiar su concepto u opinión sin que los demás se enteren y sin que esto conlleve una pérdida de imagen.

- El posible error de un concepto que tenga un experto, no será conocido ni señalado por los demás expertos.

Ciclo de repetición: Los expertos tienen la oportunidad de cambiar de opinión en otra ronda de encuesta, logrando así validar la información que brindaron o rectificándola.

En el método Delphi, (Landeta, 1999) propone distinguir dos tipos de expertos, los que denomina como “especialistas” y los “afectados”. Los primeros son los que poseen conocimiento científico y experiencia sobre la temática objeto de estudio, mientras que los segundos son los que se encuentran implicados de alguna forma en el área de estudio concreta.

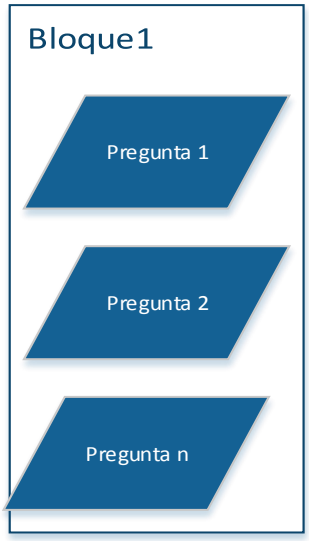
Aplicación del Método Delphi

Al inicio de la implementación del método Delphi, se contó con una base de expertos de 7 personas, al final del desarrollo de la tesis se contaba con 16 personas que alimentaron el aplicativo web, sin embargo, los datos aquí presentados muestran información inicial de 7 expertos.

Inicialmente se realizó una entrevista con cada uno de los 7 expertos y se definió una lista de chequeo a utilizar como el insumo principal para comenzar el proceso del método Delphi, de ese proceso de entrevistas surgió un banco de preguntas que se constituirían como el bloque 1 para enviar a los expertos a evaluación.

Por lo tanto, se define como el paso 1, a la recopilación del banco inicial de preguntas, ver Figura 5-1.

Figura 5-1: Bloque de preguntas para encuesta 1 (Elaboración propia)



La Tabla 5-1 muestra la información recopilada y las columnas de calificación que tienen los expertos para valorar la pregunta, de acuerdo a cinco columnas, las cuales son:

FACTOR RELEVANTE “Sí” o “No”

En este campo, el experto debe responder si considera que esa pregunta es importante para validar un control.

También se cuenta con las columnas:

- Presencia de la pregunta en el formulario
- Contenido
- Importancia
- Adecuación

En estos campos, la valoración es numérica, con una escala de Likert de 5 niveles, los cuales son:

(1) Totalmente en desacuerdo

(2) En desacuerdo

(3) Ni de acuerdo ni en desacuerdo

(4) De acuerdo

(5) Totalmente de acuerdo

Tabla 5-1: Formato de encuesta enviado de método Delphi (Elaboración propia)

FACTORES Y VARIABLES PARA SELECCIONAR CONTROLES CLAVES	FACTOR RELEVANTE "SI" O "NO"	Presencia de la pregunta en el formulario	Contenido	Importancia	Adecuación
¿LA OMISIÓN EN LA REALIZACIÓN DEL CONTROL PUEDE?					
¿Afectar la integridad de los datos?					
¿Afectar la disponibilidad de los datos?					
¿Afectar la confidencialidad de los datos?					
Afectar la efectividad de otros controles					
¿EL IMPACTO O PÉRDIDA ECONÓMICA POR LA OMISIÓN DEL CONTROL PUEDE ASCENDER A?:					
Ningún impacto económico					
Pérdida económica inferior al 0,025% del Patrimonio Contable					
Pérdida económica entre el 0,025% y el 0,15% del Patrimonio Contable					
Pérdida económica entre el 0,15% y el 0,5% del Patrimonio Contable					
Pérdida económica entre el 0,5% y el 1% del Patrimonio Contable					
Pérdida económica superior al 1% del Patrimonio Contable					
¿HISTORICAMENTE SE HAN PRESENTADO EVENTOS DE RIESGO POR LA OMISIÓN EN LA REALIZACIÓN DEL CONTROL?					
Ningún evento de riesgo					
Entre 1 y 5 eventos de riesgo					
Entre 6 y 10 eventos de riesgo					
Entre 11 y 20 eventos de riesgo					
Más de 21 eventos de riesgo					
¿EL IMPACTO O PÉRDIDA DE MERCADO POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:					
Ningún impacto en el mercado		3			
Incremento en los reclamos de algunos clientes.		2			
Incremento en los reclamos de los clientes y/o posibilidad de pérdida de clientes.					
Gran incremento en reclamos de clientes y /o alguna pérdida de estos.					
Serias pérdidas de clientes.					
Pérdida de clientes a gran escala.					

¿EL IMPACTO REPUTACIONAL POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:					
Ningún impacto reputacional					
De conocimiento a nivel de la instalación y empresa.					
De conocimiento a nivel local limitado.					
De conocimiento a nivel regional.					
De conocimiento a nivel nacional.					
De conocimiento a nivel nacional e internacional.					

¿EL IMPACTO EN EL CAPITAL HUMANO POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:					
Ningún impacto en capital humano					
Ausencia programada del personal no crítico.					
Ausencia no programada del personal no crítico.					
Ausencia programada del personal crítico u Ausencia definitiva del personal no crítico.					
Ausencia no programada del personal crítico.					
Ausencia definitiva del personal crítico.					
¿EL IMPACTO EN LOS PROCESOS POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:					
Ningún impacto en los procesos					
Intermitencias o Interrupciones en la prestación del Servicio que requieren soluciones sencillas.					
Interrupción temporal del Servicio, sin afectación de la infraestructura Física y/o tecnológica.					
Interrupción temporal del servicio, con algunas dificultades para la recuperación de la infraestructura física y/o tecnológica.					
Interrupción parcial del servicio e indisponibilidad de parte de la infraestructura física y/o tecnológica.					
Interrupción total de la prestación del servicio e indisponibilidad de la infraestructura física y tecnológica.					
¿LA POSIBILIDAD DE OCURRENCIA DE UN EVENTO OCASIONADO POR LA OMISIÓN DEL CONTROL ES?:					
Ninguna posibilidad de ocurrencia					
El evento puede ocurrir sólo bajo circunstancias excepcionales (Excepcionalmente)					
Baja posibilidad de que el evento ocurra (Pocas Veces)					
Existe una alta posibilidad de que el evento ocurra (Algunas Veces)					
El evento ocurrirá en casi cualquier circunstancia (Varias Veces)					
Se espera que el evento ocurra la mayoría de las circunstancias (Muchas Veces)					

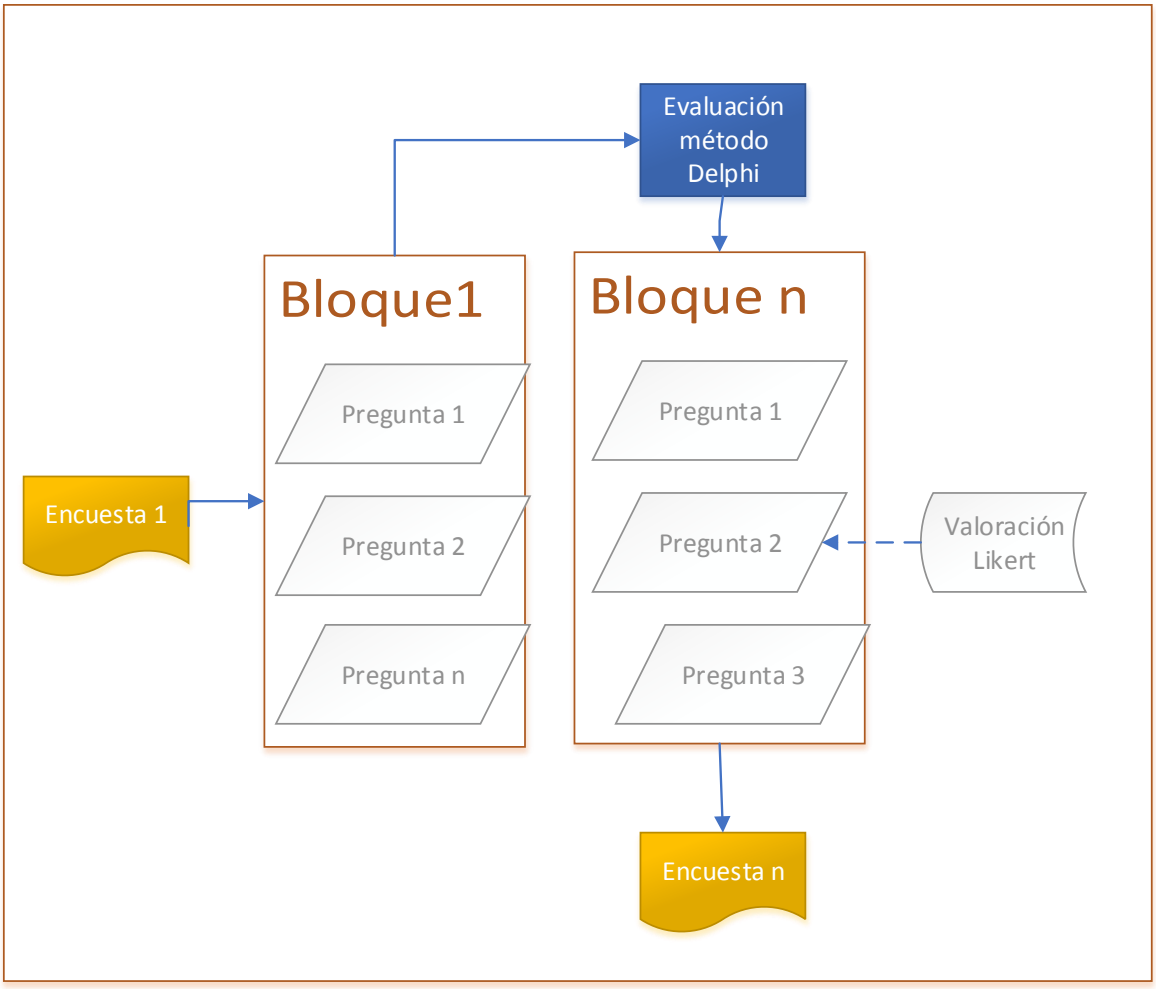
El proceso con la evaluación del método Delphi consistió en enviar por medio de correo electrónico un documento en Excel con la información descrita en la tabla 5-1, así mismo se estableció un tiempo de entrega máximo de una semana para que el libro de Excel fuera devuelto con las valoraciones y correcciones sugeridas por todos los expertos, de este modo se obtuvo el siguiente documento preliminar, ver Tabla 5-2.

Tabla 5-2: Formato de método Delphi consolidado (Elaboración propia)

FACTORES Y VARIABLES PARA SELECCIONAR CONTROLES CLAVES	Experto 1					Experto 2					
	FACTOR RELEVANTE "SI" O "NO"	Presencia de la pregunta en el formulario	Contenido	Importancia	Adecuación	FACTOR RELEVANTE "SI" O "NO"	Presencia de la pregunta en el formulario	Contenido	Importancia	Adecuación	FACTOR RELEVANTE "SI" O "NO"
¿LA OMISIÓN EN LA REALIZACIÓN DEL CONTROL PUEDE?											
¿Afectar la integridad de los datos?	Sí	(5) Totalmente de acuerd	(4) De acuerd	(5) Totalmente de acue	(4) De acuerdo	Sí	(5) Totalmente de a	(4) De acuerdo	(4) De acuerdo	(4) De acuerdo	Sí
¿Afectar la disponibilidad de los datos?	Sí	(5) Totalmente de acuerd	(4) De acuerd	(5) Totalmente de acue	(4) De acuerdo	Sí	(5) Totalmente de a	(4) De acuerdo	(4) De acuerdo	(4) De acuerdo	Sí
¿Afectar la confidencialidad de los datos?	Sí	(5) Totalmente de acuerd	(4) De acuerd	(5) Totalmente de acue	(4) De acuerdo	Sí	(5) Totalmente de a	(4) De acuerdo	(4) De acuerdo	(4) De acuerdo	Sí
Afectar la efectividad de otros controles	NO	(2) En desacuerdo	(2) En desacu	(2) En desacuerdo	(2) En desacuer	Sí	(5) Totalmente de a	(4) De acuerdo	(4) De acuerdo	(4) De acuerdo	NO
¿EL IMPACTO O PÉRDIDA ECONÓMICA POR LA OMISIÓN DEL CONTROL PUEDE ASCENDER A?:											
Ningún impacto económico	Sí	(2) En desacuerdo	(2) En desacu	(2) En desacuerdo	(2) En desacuer	Sí	(5) Totalmente de a	(2) En desacu	(4) De acuerdo	(2) En desacuer	Sí
Pérdida económica inferior al 0,025% del Patrimonio Contable	No	(2) En desacuerdo	(2) En desacu	(2) En desacuerdo	(2) En desacuer	Sí	(5) Totalmente de a	(2) En desacu	(4) De acuerdo	(2) En desacuer	No
Pérdida económica entre el 0,025% y el 0,15% del Patrimonio Contable	No	(2) En desacuerdo	(2) En desacu	(2) En desacuerdo	(2) En desacuer	Sí	(5) Totalmente de a	(2) En desacu	(4) De acuerdo	(2) En desacuer	No
Pérdida económica entre el 0,15% y el 0,5% del Patrimonio Contable	No	(2) En desacuerdo	(2) En desacu	(2) En desacuerdo	(2) En desacuer	Sí	(5) Totalmente de a	(2) En desacu	(4) De acuerdo	(2) En desacuer	No
Pérdida económica entre el 0,5% y el 1% del Patrimonio Contable	No	(2) En desacuerdo	(2) En desacu	(2) En desacuerdo	(2) En desacuer	Sí	(5) Totalmente de a	(2) En desacu	(4) De acuerdo	(2) En desacuer	No
Pérdida económica superior al 1% del Patrimonio Contable	Sí	(2) En desacuerdo	(2) En desacu	(2) En desacuerdo	(2) En desacuer	Sí	(5) Totalmente de a	(2) En desacu	(4) De acuerdo	(2) En desacuer	Sí
RIESGO POR LA OMISIÓN EN LA REALIZACIÓN DEL CONTROL?											
Ningún evento de riesgo	Sí	(2) En desacuerdo	(5) Totalmente	(5) Totalmente de acue	(5) Totalmente d	Sí	(5) Totalmente de a	(5) Totalmente	(5) Totalmente	(5) Totalmente d	No
Entre 1 y 5 eventos de riesgo	Sí	(1) Totalmente en desacu	(2) En desacu	(3) Ni de acuerdo ni en	(1) Totalmente e	No	(2) En desacuerdo	(2) En desacu	(2) En desacue	(2) En desacuer	No
Entre 6 y 10 eventos de riesgo	Sí	(1) Totalmente en desacu	(2) En desacu	(3) Ni de acuerdo ni en	(1) Totalmente e	No	(2) En desacuerdo	(2) En desacu	(2) En desacue	(2) En desacuer	No
Entre 11 y 20 eventos de riesgo	Sí	(1) Totalmente en desacu	(2) En desacu	(3) Ni de acuerdo ni en	(1) Totalmente e	No	(2) En desacuerdo	(2) En desacu	(2) En desacue	(2) En desacuer	No
Más de 21 eventos de riesgo	No	(1) Totalmente en desacu	(2) En desacu	(3) Ni de acuerdo ni en	(1) Totalmente e	No	(2) En desacuerdo	(2) En desacu	(2) En desacue	(2) En desacuer	No
¿EL IMPACTO O PÉRDIDA DE MERCADO POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:											
Ningún impacto en el mercado	Sí	(5) Totalmente de acuerd	(5) Totalmente	(5) Totalmente de acue	(5) Totalmente d	Sí	(5) Totalmente de a	(5) Totalmente	(5) Totalmente	(5) Totalmente d	Sí
Incremento en los reclamos de algunos clientes.	No	(2) En desacuerdo	(2) En desacu	(2) En desacuerdo	(2) En desacuer	Sí	(1) Totalmente en d	(1) Totalmente	(1) Totalmente	(1) Totalmente e	Sí
Incremento en los reclamos de los clientes y/o posibilidad de pérdida de clientes.	Sí	(2) En desacuerdo	(2) En desacu	(2) En desacuerdo	(2) En desacuer	Sí	(2) En desacuerdo	(2) En desacu	(2) En desacue	(2) En desacuer	Sí
Gran incremento en reclamos de clientes y/o alguna pérdida de estos	Sí	(2) En desacuerdo	(2) En desacu	(2) En desacuerdo	(2) En desacuer	Sí	(2) En desacuerdo	(2) En desacu	(2) En desacue	(2) En desacuer	Sí

De esta manera, como se observa en la Figura 5-2 el proceso arroja una encuesta nueva después de ser agregadas las sugerencias de los expertos.

Figura 5-2: Modelo de evaluación Delphi (Elaboración propia)



Cada experto tiene un peso es su evaluación, de acuerdo a las variables que se tuvieron en cuenta en el momento de seleccionar el experto, dichas variables son, ver tabla 5-3:

Tabla 5-3: Variable de calificación de perfil de experto (Elaboración propia)

Años de experiencia en el ejercicio profesional
Nivel de formación académica
Sector económico donde labora
Título profesional
Certificación

De acuerdo a cada variable, se tiene un puntaje asignado, así cada una de las variables tiene en cuenta lo siguiente, ver Tabla 5-4, Tabla 5-5, Tabla 5-6, Tabla 5-7, Tabla 5-8:

Tabla 5-4: Escala Likert de variable años de experiencia (Elaboración propia)

Años de experiencia en el ejercicio profesional	**Puntaje**
Sin experiencia	**0**
Practicante	**1**
1 a 3 años	**2**
De 4 a 7 años	**3**
De 8 a 12 años	**4**
Más de 12 años	**5**

Tabla 5-5: Escala Likert de variable nivel de formación (Elaboración propia)

Nivel de formación académica	**Puntaje**
Técnico	**1**
Tecnólogo	**1**
Profesional	**3**
Especialista	**3**
Maestría	**4**
Doctorado	**5**

Tabla 5-6: Escala Likert de variable sector económico (Elaboración propia)

Sector económico donde labora	**Puntaje**
Sector agropecuario	**2**
Sector de servicios	**4**
Sector industrial	**3**
Sector de transporte	**3**
Sector financiero	**5**
Sector de la construcción	**3**
Sector minero y energético	**5**
Sector solidario	**4**
Sector de comunicaciones	**5**

Tabla 5-7: Escala Likert de variable título profesional (Elaboración propia)

Título profesional	Puntaje
Ingeniero de Sistemas o afines	**5**
Abogado	**3**
Contador público	**3**
Economista	**3**
Ingeniero Industrial	**5**
Ingeniero de Calidad	**5**

Tabla 5-8: Escala Likert de variable certificación (Elaboración propia)

Certificación	Puntaje
No tiene	**0**
ISO/IEC 27001 Provisional Auditor	**3**
ISO/IEC 27001 Auditor	**4**
ISO/IEC 27001 Lead Auditor	**5**

Dentro de las consideraciones de variables, inicialmente se contaba con el cargo, sin embargo, ya que en Colombia no se cuenta con un estándar de niveles de jerarquía en los cargos, se optó por omitir dicha variable.

De acuerdo a la valoración de las tablas anteriores, se asigna un peso a cada experto, ver la Tabla 5-9, con las características de los expertos.

Tabla 5-9: Pesos y características de los expertos evaluadores (Elaboración propia)

	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Experto 6	Experto 7
Años de experiencia en el ejercicio profesional	2	2	3	5	3	4	3
Nivel de formación académica	3	4	3	4	3	3	4
Sector económico donde labora	4	4	4	5	4	5	5

Título profesional	3	4	3	5	3	5	3
Certificaciones	4	3	4	5	4	4	4
Puntaje Promedio	3,2	3,4	3,4	4,8	3,4	4,2	3,8
Peso de la evaluación del experto %	12,2	13,0	13,0	18,3	13,0	16,0	14,5

Se obtiene un puntaje promedio de cada experto, la suma de esos puntajes será la base del 100% para calcular el peso de la evaluación de experto en porcentaje.

Dentro de todo el proceso del método Delphi, y como se pudo ver en la Figura 5-2, las iteraciones de las encuestas terminan cuando se tiene una valoración de criterios por parte de los expertos con alfa de Cronbach >=0.7 ver Tabla 5-10, en este punto, indica que se tiene un elevado consenso entre los expertos (Frías Navarro, 2014). De este modo la encuesta 'n' termina, para este caso de siete expertos, ver Figura 5-3.

La estimación de confiabilidad que se puede encontrar mediante el alfa de Cronbach asume que los ítems (medidos en escala tipo Likert o también es posible para ítems dicotómicos) miden un bloque de valores y que están altamente correlacionados entre sí. Al menos se necesitan dos ítems para poder estimar el valor del coeficiente alfa de Cronbach y cuanto mayor el número de ítems mayor será la fiabilidad de la escala (Landeta, 1999).

La ecuación (5.1)(Cronbach, 1951) indica el cálculo del estimador Alfa de Cronbach.

Tabla 5-10: Escala de valoración Alfa de Cronbach (Frías Navarro, 2014)

Alfa	**Evaluación**
<0,70	No se acepta
>0,70 y <0,86	Aceptable
>=0,86	Notable de aceptación

$$\propto = \frac{K}{K-1}\left[1 - \frac{\sum s_i^2}{s_T^2}\right] \qquad (5.1)$$

Donde:

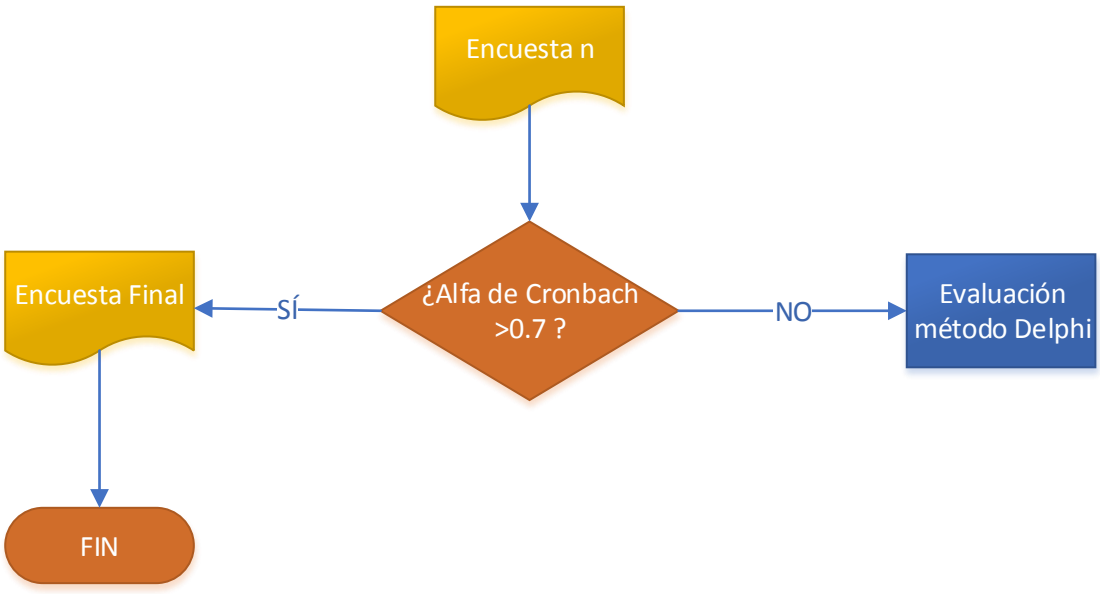
K: El número de ítems

s_i^2: Sumatoria de Varianzas de los Ítems

s_T^2: Varianza de la suma de los Ítems

$\propto$: Coeficiente de Alfa de Cronbach

Figura 5-3: Proceso de comparación Alfa Cronbach (Elaboración propia)



Después de realizado el proceso de selección de las preguntas para la encuesta, es necesario asignar los pesos a las preguntas y variables de respuesta que tienen.

En la Figura 5-4 se observa la estructura del cuestionario, de acuerdo a lo siguiente:

El rectángulo rojo señala lo que se determinó se llama un bloque, este bloque consiste de varias preguntas o una pregunta con única selección, el cuadro azul señala el peso que se le da a esa variable o pregunta, el cuadro amarillo señala el peso que tiene ese

bloque de preguntas en toda la encuesta, para el caso de ejemplo, el bloque representa el 20% del total del cuestionario.

Figura 5-4: Estructura del cuestionario de calificación de control (Elaboración propia)

FACTORES Y VARIABLES PARA SELECCIONAR CONTROLES CLAVES			Peso de variable porcentaje
¿LA OMISIÓN EN LA REALIZACIÓN DEL CONTROL PUEDE?	Respuesta	Peso de variable %	10%
¿Afectar la integridad de los datos?		33,33	
¿Afectar la disponibilidad de los datos?	x	33,33	
¿Afectar la confidencialidad de los datos?		33,33	
¿EL IMPACTO O PERDIDA ECONOMICA POR LA OMISION DEL CONTROL PUEDE ASCENDER A?:	Elección		20%
Ningún impacto económico		0	
Pérdida económica inferior al 0,025% del Patrimonio Contable		50%	
Pérdida económica entre el 0,025% y el 0,15% del Patrimonio Contable		65%	
Pérdida económica entre el 0,15% y el 0,5% del Patrimonio Contable		85%	
Pérdida económica entre el 0,5% y el 1% del Patrimonio Contable	x	100%	

Para asignar los pesos se realizó nuevamente el proceso de evaluación Delphi ilustrado en la figura Figura 5-4, se requieren los pesos de cada variable y el peso de cada bloque, para esto fueron consultados nuevamente los expertos y se llegó al documento final, ver Tabla 5-11

Tabla 5-11: Calificación y resultado de control de SGSI (Elaboración propia)

	FACTORES Y VARIABLES PARA SELECCIONAR CONTROLES CLAVES			Peso de variable porcentaje	Peso de variable en puntos	Porcentaje calculado	Resultado: Porcentaje del bloque para el control	Resultado: Puntaje del bloque para el control
1	¿LA OMISIÓN EN LA REALIZACIÓN DEL CONTROL PUEDE?	Respuesta	Peso de variable %	10%	0,5	33%	3%	0,16665
	¿Afectar la integridad de los datos?		33,33					
	¿Afectar la disponibilidad de los datos?	x	33,33					
	¿Afectar la confidencialidad de los datos?		33,33					
2	¿EL IMPACTO O PERDIDA ECONOMICA POR LA OMISION DEL CONTROL PUEDE ASCENDER A?:	Elección		20%	1	100%	20%	1
	Ningún impacto económico		0					
	Pérdida económica inferior al 0,025% del Patrimonio Contable		50%					
	Pérdida económica entre el 0,025% y el 0,15% del Patrimonio Contable		65%					
	Pérdida económica entre el 0,15% y el 0,5% del Patrimonio Contable		85%					
	Pérdida económica entre el 0,5% y el 1% del Patrimonio Contable	x	100%					
3	¿HISTORICAMENTE SE HAN PRESENTADO EVENTOS DE RIESGO POR LA OMISIÓN EN LA REALIZACIÓN DEL CONTROL?			10%	0,5	100%	10%	0,5
	Ningún evento de riesgo		0%					
	Entre 1 y 5 eventos de riesgo		50%					
	Entre 6 y 10 eventos de riesgo		65%					
	Entre 11 y 20 eventos de riesgo		90%					
	Más de 21 eventos de riesgo	x	100%					
4	¿EL IMPACTO O PERDIDA DE MERCADO POR LA OMISION DEL CONTROL PUEDE REPRESENTAR?:			10%	0,5	100%	10%	0,5
	Ningún impacto en el mercado		0%					
	Incremento en los reclamos de algunos clientes.		10%					
	Incremento en los reclamos de los clientes y/o posibilidad de pérdida de clientes.		60%					
	Gran incremento en reclamos de clientes y /o alguna pérdida de estos.		75%					
	Serias pérdidas de clientes.		90%					
	Pérdida de clientes a gran escala.	x	100%					
5	¿EL IMPACTO REPUTACIONAL POR LA OMISION DEL CONTROL PUEDE REPRESENTAR?:			10%	0,5	100%	10%	0,5
	Ningún impacto reputacional		0%					
	De conocimiento a nivel de la instalación y empresa.		40%					
	De conocimiento a nivel local limitado.		45%					
	De conocimiento a nivel regional.		65%					
	De conocimiento a nivel nacional.		95%					
	De conocimiento a nivel nacional e internacional.	x	100%					
6	¿EL IMPACTO EN EL CAPITAL HUMANO POR LA OMISION DEL CONTROL PUEDE REPRESENTAR?:			20%	1	100%	20%	1
	Ningún impacto en capital humano		0%					
	Ausencia programada del personal no crítico.		10%					
	Ausencia no programada del personal no crítico.		35%					
	Ausencia programada del personal crítico u Ausencia definitiva del personal no crítico.		55%					
	Ausencia no programada del personal crítico.		85%					
	Ausencia definitiva del personal crítico.	x	100%					
7	¿EL IMPACTO EN LOS PROCESOS POR LA OMISION DEL CONTROL PUEDE REPRESENTAR?:			10%	0,5	65%	7%	0,325
	Ningún impacto en los procesos		0					
	Intermitencias o Interrupciones en la prestación del Servicio que requieren soluciones sencillas.		5%					
	Interrupción temporal del Servicio, sin afectación de la infraestructura Física y/o tecnológica.		10%					
	Interrupción temporal del servicio, con algunas dificultades para la recuperación de la infraestructura física y/o tecnológica.		30%					
	Interrupción parcial del servicio e indisponibilidad de parte de la infraestructura física y/o tecnológica.	x	65%					
	Interrupción total de la prestación del servicio e indisponibilidad de la infraestructura física y tecnológica.		100%					
8	¿LA POSIBILIDAD DE OCURRENCIA DE UN EVENTO OCASIONADO POR LA OMISIÓN DEL CONTROL ES?:			10%	0,5	100%	10%	0,5
	Ninguna posibilidad de ocurrencia		0%					
	El evento puede ocurrir sólo bajo circunstancias excepcionales (Excepcionalmente)		5%					
	Baja posibilidad de que el evento ocurra (Pocas Veces)		25%					
	Existe una alta posibilidad de que el evento ocurra (Algunas Veces)		55%					
	El evento ocurrirá en casi cualquier circunstancia (Varias Veces)		85%					
	Se espera que el evento ocurra la mayoría de las circunstancias (Muchas Veces)	x	100%					
							Puntaje para el control	4,49

De acuerdo al puntaje para el control obtenido en el cálculo, se realiza la clasificación para el control, teniendo en cuenta el estándar CVSS - Common Vulnerability Scoring

System, el cual asigna puntuaciones de gravedad a las vulnerabilidades en seguridad de la información (Mell, Scarfone, & Romanosky, 2007), ver Tabla 5-12.

La clasificación está dada por los siguientes conceptos:

Nulo: No existe riesgo

Bajo: Si se llega a materializar un riesgo asociado a un control que está calificado como bajo, el impacto es casi nulo o insignificante y pueden ser erradicadas por completo con la primera detección.

Medio: El impacto de clasificación medio es considerable en recursos y en información, sin embargo, estos recursos e información se consideran como no críticos, información no relevante.

Alto: Este impacto alto, se considera como delicado, aunque no muy significativo en recursos que se clasifican como críticos, amenazando una cantidad limitada de sistemas que se consideran no críticos.

Crítico: Este es el mayor impacto, en él se incluyen vulnerabilidades o intrusiones a la información clasificada de la compañía, afectando la confidencialidad, disponibilidad o la integridad de los datos.

Tabla 5-12: Clasificación de resultados CVSS (FIRST, 2015)

Clasificación	CVSS Score
Nulo	0
Bajo	0.1 – 1.99
Medio	2 – 3.49
Alto	3.5 – 4.49
Crítico	4.5 - 5

5.2 Prototipo para evaluación de controles

En este punto, el trabajo se realizó con una base de datos de conocimiento de 7 expertos, sin embargo, se pretende que el número no sea limitado, por lo que tomamos la iniciativa de desarrollar un prototipo de aplicación web, que nos permitiera aplicar todo el proceso de evaluación Delphi hasta el proceso que se debe realizar para poner un control en evaluación.

Se desarrolló una aplicación web la cual fue denominada ISOWEB, fue implementada en el framework de desarrollo php Laravel, con la firme intención de ser una plataforma libre, totalmente opensource bajo una licencia GPL v2.

El alcance de la aplicación, requiere que previamente se hayan realizado los análisis de riesgos latentes que hay en la organización, posteriormente se podrá hacer uso de la aplicación, en la Figura 5-5 se observa la pantalla inicial en la cual un usuario podría registrarse a ingresar, siendo un evaluador experto o un auditor que usará la aplicación como usuario final, es por ello que en la Figura 5-6 se observa el formulario de preguntas que corresponden a la perfil del experto, para asignarle los pesos correspondientes que formarán la base de conocimiento de la encuesta.

Figura 5-5: Pantalla inicial (Elaboración propia)

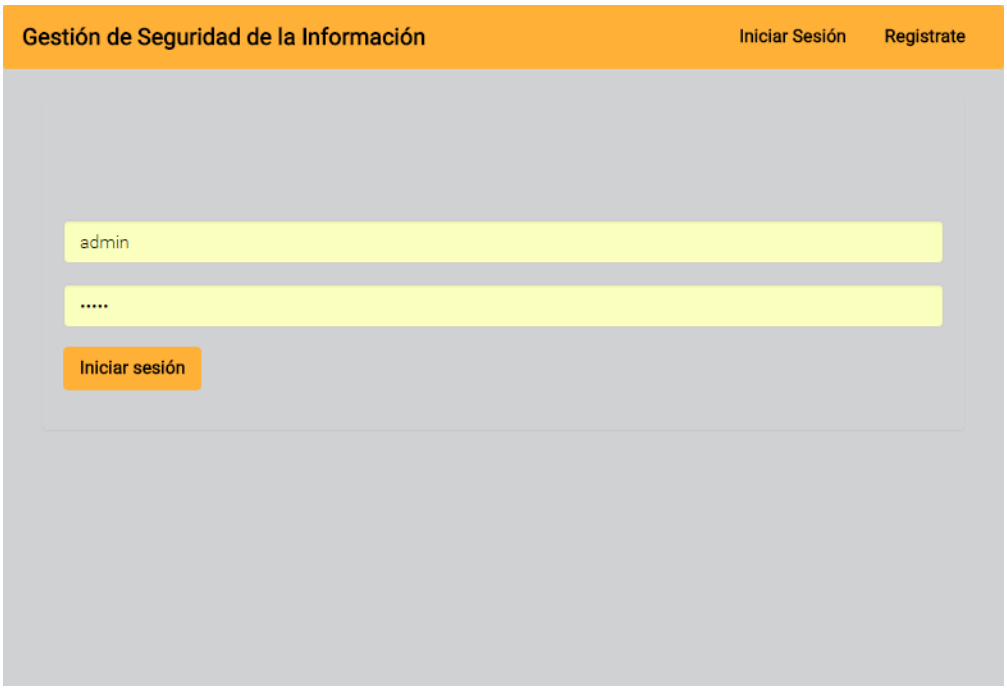
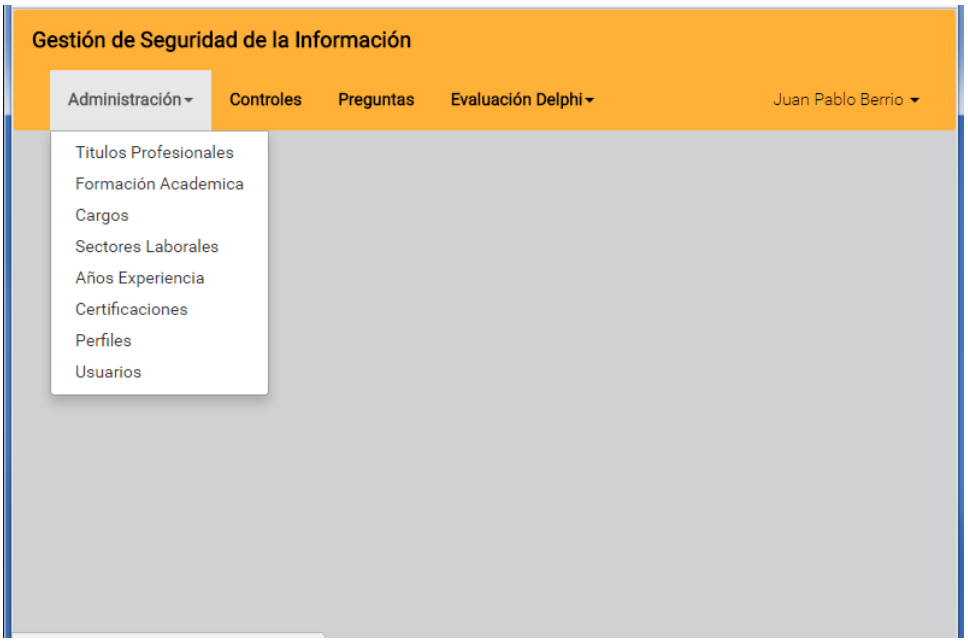


Figura 5-6: Registro de experto (Elaboración propia)

De acuerdo a la Tabla 5-3, en la Figura 5-7 se puede observar las secciones diferentes en las cuales se encuentras dichas variables, que pueden modificarse a medida en que se reciba retroalimentación o el diseño de la aplicación cambie.

Figura 5-7: Secciones de variables creadas (Elaboración propia)



En la Figura 5-8 se observan los valores ingresados en la variable título profesional, se conserva el mismo formato para las demás variables, en las cuales se puede agregar nuevos registros, se pueden modificar o establecer un estado de activado o desactivado.

Figura 5-8: Variable títulos profesionales (Elaboración propia)

La Figura 5-9 presenta los controles del estándar ISO/IEC 27001 registrados, cada control tiene la opción de editarlo, de seleccionar las preguntas que tendrá asociadas si es que no todas las preguntas de la encuesta aplican para ese control y por último el ícono de check lleva al proceso de responder las preguntas, dichas preguntas deben ser previamente agregadas, como se ve en la Figura 5-10.

Figura 5-9: Controles agregados para evaluación (Elaboración propia)

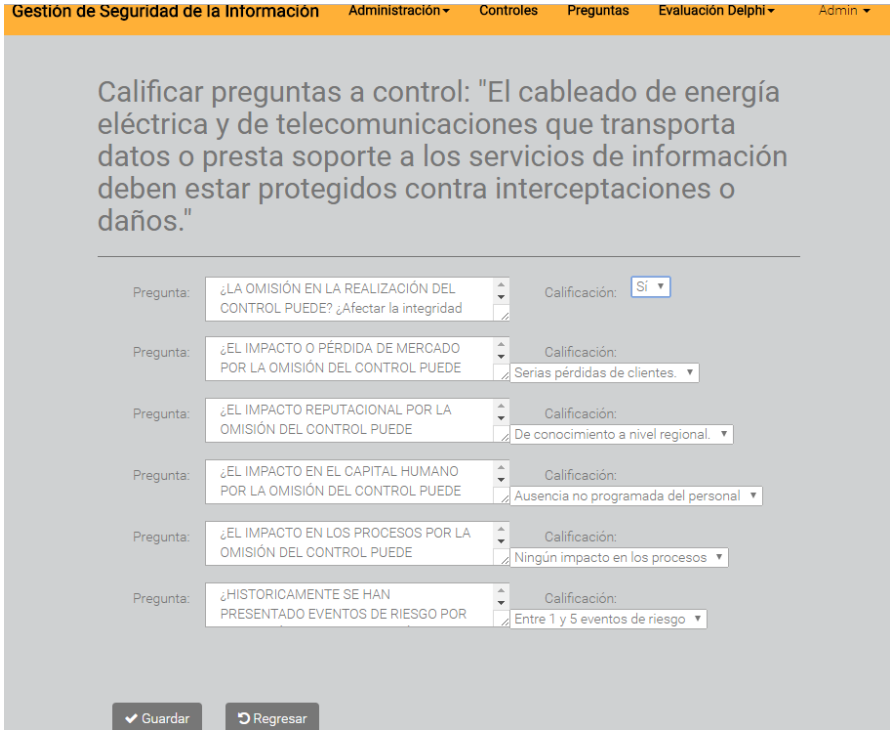
Figura 5-10: Preguntas registradas para evaluación (Elaboración propia)

Una de las grandes ventajas de trasladar todo el proceso a una aplicación, es la posibilidad de que a medida que un usuario se registre, se incrementará la base de conocimiento, lo nos dará una confiabilidad mayor cada que se agrega la valoración de un experto a la encuesta. En la Figura 5-11 se puede ver el peso que tendrá ese experto en particular, y de acuerdo a su calificación tendrá un 14% de relevancia sobre sus opiniones en la encuesta.

Figura 5-11: Valoración y peso que se le dio al experto (Elaboración propia)

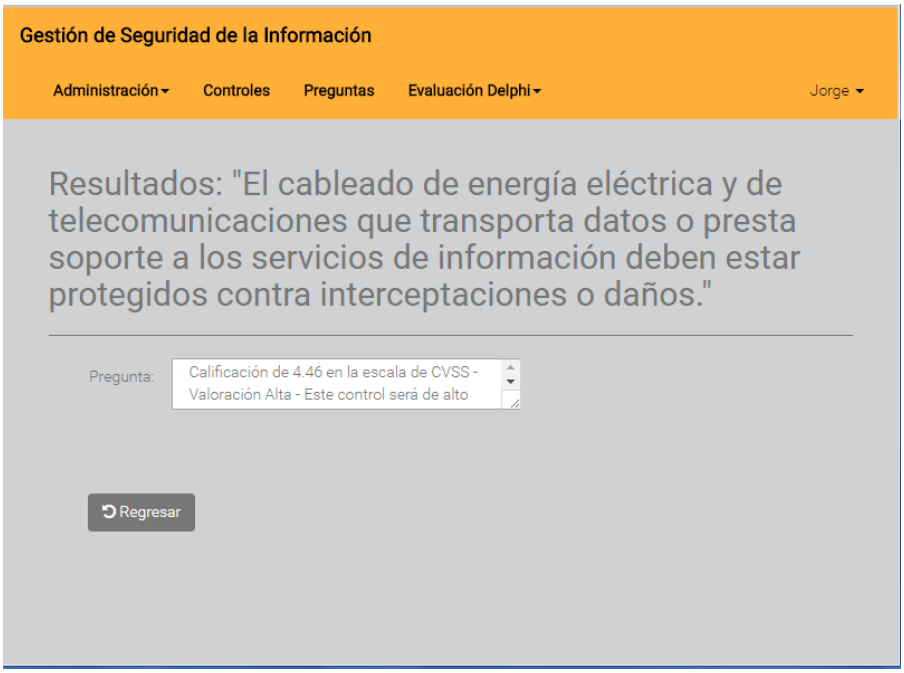
En la Figura 5-12, se puede observar cómo se realiza la calificación de un control en un bloque de preguntas, dependiendo del tipo de pregunta, la aplicación notificará el valor en la escala de Likert.

Figura 5-12: Calificación de preguntas asociadas a control (Elaboración propia)



La Figura 5-13, se muestra el resultado de la evaluación a un control, con la recomendación de implementación para el SGSI.

Figura 5-13: Resultado de valoración de un control (Elaboración propia)



5.3 Caso de Estudio

El prototipo y toda la metodología fue puesta a disposición del área de riesgo de una compañía de financiamiento, en la compañía ya tenían implementado un SGSI sin certificar, ya existe la figura de oficial de seguridad de la información, y es él quien se encarga de implementarlo y de auditarlo, por lo que es un perfil que está mal definido, ya que no debe auditarlo internamente quien implementa las normas, de acuerdo a lo anterior, en forma mancomunada, se realizó el proceso de verificar todos los controles de la norma colombiana NTC ISO/IEC 27001(International Organization for Standardization, 2013b), con la encuesta definida por el panel de expertos de esta investigación y de ese modo obtener la calificación de cada control respecto a las necesidades de la compañía, este trabajo se realizó durante 6 meses, como prueba piloto, por lo que se inició el proceso de tomar uno por uno, evaluarlo y se obtuvo el resultado siguiente en cada control, ver Tabla 5-13.

Tabla 5-13: Controles evaluados en compañía de financiamiento (Elaboración propia)(International Organization for Standardization, 2013b)

CONTROLES ISO/IEC 27001	Puntaje de Control
Política de seguridad de la información	
La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.	3,47
La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.	2,10
Organización interna	
La dirección debe apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información.	3,94
Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes de la organización con roles y funciones laborales pertinentes.	4,05
Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información.	3,05
Se debe definir e implementar un proceso de autorización de la dirección para nuevos servicios de procesamiento de información.	3,95
Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.	3,00
Se deben mantener contactos apropiados con las autoridades pertinentes.	3,84
Se deben mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales	4,06
El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.	3,61
Partes externas	

Se deben identificar los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.	2,10
Todos los requisitos de seguridad identificados se deben considerar antes de dar acceso a los clientes a los activos o la información de la organización	3,00
Los acuerdos con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los requisitos pertinentes de seguridad	2,84
Toda la información y los activos asociados con los servicios de procesamiento de información deben ser "propiedad"3) de una parte designada de la organización	4,02
Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información	4,09
Clasificación de la información	
La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.	3,30
Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización	2,16
SEGURIDAD DE LOS RECURSOS HUMANOS	
Se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización	3,69
Se deben realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos	4,97
Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus	3,80

responsabilidades y las de la organización con relación a la seguridad de la información.	
La dirección debe exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización.	3,61
Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.	4,04
Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad	3,69
Terminación o cambio de la contratación laboral	
Se deben definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.	4,84
Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.	4,25
Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio.	2,45
SEGURIDAD FÍSICA Y DEL ENTORNO	
Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información	2,54
Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	3,39
Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	2,01
Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	2,30
Se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.	4,82

Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deben controlar y, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.	2,30
Seguridad de los equipos	
Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado	2,52
Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.	3,48
El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información deben estar protegidos contra interceptaciones o daños.	3,85
Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	4,41
Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	4,43
Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.	2,45
Ningún equipo, información ni software se deben retirar sin autorización previa.	4,61
GESTIÓN DE COMUNICACIONES Y OPERACIONES	
Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	3,50
Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información.	2,31
Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.	3,06
Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.	4,00
Gestión de la prestación del servicio por terceras partes	

Se deben garantizar que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes.	4,42
Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares.	2,68
Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.	4,23
Planificación y aceptación del sistema	
Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.	2,74
Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.	2,27
Protección contra códigos maliciosos y móviles	
Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.	3,72
Cuando se autoriza la utilización de códigos móviles, la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se debe evitar la ejecución de los códigos móviles no autorizados.	4,07
Respaldo	
Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.	3,71
Gestión de la seguridad de las redes	

Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.	4,09
En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente.	2,19
Manejo de los medios	
Se deben establecer procedimientos para la gestión de los medios removibles	4,61
Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin riesgo, utilizando los procedimientos formales.	3,91
Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	3,55
La documentación del sistema debe estar protegida contra el acceso no autorizado.	2,71
Intercambio de la información	
Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.	4,35
Se deben establecer acuerdos para el intercambio de la información y del software entre la organización y partes externas.	4,29
Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.	3,34
La información contenida en la mensajería electrónica debe tener la protección adecuada	2,80
Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio.	2,93
Servicios de comercio electrónico	
La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada.	3,37

La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.	2,23
La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.	4,78
Monitoreo	
Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.	3,24
Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad	3,80
Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.	4,52
Se deben registrar las actividades tanto del operador como del administrador del sistema.	2,12
Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.	3,80
Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.	3,92
CONTROL DE ACCESO	
Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso	3,95
Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.	2,86
Se debe restringir y controlar la asignación y uso de privilegios.	3,40
La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.	4,85
La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.	3,93
Responsabilidades de los usuarios	

Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.	2,99
Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	3,17
Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.	2,77
Control de acceso a las redes	
Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.	4,50
Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	2,56
La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.	3,68
El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado	3,35
En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.	4,55
Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación del negocio	3,50
Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio.	3,90
Control de acceso al sistema operativo	
El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.	2,15
Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.	2,59
Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	2,15
Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.	4,48

Las sesiones inactivas se deben suspender después de un periodo definido de inactividad.	4,70
Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo	3,26
Control de acceso a las aplicaciones y a la información	
Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.	2,19
Los sistemas sensibles deben tener un entorno informático dedicado (aislados).	2,90
Computación móvil y trabajo remoto	
Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	4,74
Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.	2,42
Requisitos de seguridad de los sistemas de información	
Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.	4,15
Procesamiento correcto en las aplicaciones	
Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados	4,43
Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.	3,75
Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.	3,44
Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias	3,02
Controles criptográficos	

Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	4,67
Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.	4,54
Seguridad de los archivos del sistema	
Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	4,26
Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse.	2,27
Se debe restringir el acceso al código fuente de los programas.	4,92
Seguridad en los procesos de desarrollo y soporte	
Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.	2,85
Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.	3,66
Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	4,89
Se deben evitar las oportunidades para que se produzca fuga de información.	3,14
La organización debe supervisar y monitorear el desarrollo de software contratado externamente.	4,61
Gestión de la vulnerabilidad técnica	
Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	4,65
Reporte sobre los eventos y las debilidades de la seguridad de la información	
Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.	2,55

Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.	3,51
Gestión de los incidentes y las mejoras en la seguridad de la información	
Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	3,63
Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.	2,13
Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.	3,32
Aspectos de seguridad de la información, de la gestión de la continuidad del negocio	
Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	4,15
Se deben identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.	2,78
Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio.	4,85
Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento	2,24
Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia	2,21
Cumplimiento de los requisitos legales	

Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización	2,76
Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	2,41
Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.	3,93
Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.	2,24
Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.	4,82
Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.	3,33
Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico	
os directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.	2,99
Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.	4,19
Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.	2,51
Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.	3,95

De acuerdo a la recolección de la información anterior, se obtuvo la Tabla 5-14 de clasificación de los controles

Tabla 5-144: Clasificación por cantidad de controles (Elaboración propia)

Clasificación	Cantidad Controles
Medio	63
Alto	49
Crítico	20

Con base en lo anterior, 63 controles fueron clasificados con un impacto Medio, los impactos medios deben notificarse con un tiempo máximo de una semana y su erradicación, solución, corrección, debe llevarse a acabo en un mes.

Con impacto alto, fueron clasificados 49 controles, que implican una notificación de 24 horas, y una solución, corrección de 4 a 5 días desde el momento de su detección.

El nivel de clasificación más alto llamado crítico, fue alcanzado por 20 controles, los cuales requieren máxima prioridad, ya que, con la materialización de los riesgos asociados a ellos, se puede acceder a información confidencial, que puede poner en peligro la estabilidad del negocio. Los controles considerados como críticos deben ser reportados en máximo una hora y deben ser tratados en las próximas 8 horas desde la detección de la necesidad de implementarlos.

Esta prueba de calificación de controles en la compañía de financiamiento , sirvió para elevar los niveles de alerta desde el área de seguridad, ya que el SGSI que se había implementado no ha sido certificado y por ellos muchos riesgos no han sido plenamente identificados y muchos de los controles no tienen la prioridad que requieren, desde el mes de agosto de 2016, inició el trabajo de validar uno a uno los controles clasificados como críticos, este trabajo se valida con el área de implementación de tecnología inicialmente, y será el oficial de seguridad quien realice la auditoría.

6. Conclusiones y recomendaciones

6.1 Conclusiones

Para lograr una efectiva implementación de un Sistema de Gestión de Seguridad de Información, se recomienda contar con el concepto de varios expertos que puedan evaluar tanto el análisis de riesgos realizado previamente a la implementación como los controles seleccionados para dicha implementación.

El método Delphi es una herramienta muy útil para consolidar información que puede ser sensible cuando sólo se tiene un punto de vista, con el ejercicio realizado en este trabajo se demostró que se puede lograr un consenso rápidamente siempre y cuando las personas involucradas en el proceso, tengan mucha afinidad en el tema de trabajo, lo que permite que no se discuta el porqué de los conceptos si no el cómo.

El conocimiento y experiencia de los expertos es el principal insumo para poder realizar una valoración y calificación de los controles de seguridad de la información, pero se recalca que, para este trabajo, tuvo relevancia si se realizó de manera conjunta la evaluación logrando unificar opiniones, ya que, si no se cumple con este propósito, se estaría incurriendo nuevamente en una valoración más subjetiva.

El proceso de análisis de riesgos, debe convocar a todas las áreas de una organización, aún más hablando de seguridad de la información, no es un tema que competa sólo al área de tecnología, pues los empleados deben ser los primeros es saber detectar cuando se tiene un riesgo de seguridad.

La implementación de un SGSI requiere estar a la vanguardia de las innovaciones tecnológicas, en este aspecto, el área de tecnología sí tiene un papel muy destacado, ya que debe proponer herramientas metodológicas tanto para la prevención como para la detección de riesgos relacionados con el aumento de vulnerabilidades informáticas, teniendo en cuenta que la mayoría de áreas de una compañía está conectada a la red.

Una de las principales desventajas o problemas que tienen las opiniones de los expertos en un proceso de auditoría, consiste en que no conocen bien el proceso que auditan, como

es el caso de auditor los sistemas de información, ya que si se da el caso de tener un auditor con un perfil profesional más orientado a los procesos, no conocerá a fondo del funcionamiento técnico de los sistema usados y cómo pueden ser vulnerables, por ello es importante destacar que las organizaciones deben formalizar el cargo del llamada Oficial de seguridad de la información, como un perfil integral y transversal a todos los procesos de la compañía, logrando además de identificar riesgos, proponer soluciones.

El insumo del prototipo desarrollado, puede usarse no solamente para sistemas de gestión de seguridad, pues las organizaciones se ven hoy en día sujetas a regulaciones o estatutos nacionales que deben revisar constantemente, por lo cual se constituyen en candidatos para ser valorados internamente mediante la implementación de controles, que pueden ser objeto de evaluación de la presente metodología.

Todas las organizaciones y personas viven expuestas a algún tipo de riesgo de seguridad de la información, recordando que no sólo es la información digital, es importante que la prevención esté presente siempre en las medidas tomadas como controles de seguridad, y que la corrección se realice mediante una gestión proactiva y no a raíz de una materialización de un riesgo.

Si bien, las organizaciones internacionales de auditoría tienen sus propios métodos para medir los controles y el desempeño que podrían tener estos en un SGSI, la implementación de la metodología propuesta puede ser adaptada a un nuevo modelo de evaluación de acuerdo a los requerimientos del auditor líder, ya que el propósito de todo este proceso es servir al mejoramiento continuo, orientado al desarrollo del negocio y nuevas estrategias para la consecución de metas.

6.2 Recomendaciones

Partiendo de las recomendaciones recibidas por parte de los expertos consultados, estas pueden encaminarse en dos trabajos, todo el proceso de la manera en que son consultados los expertos y el desarrollo de la aplicación.

Se propone que la encuesta enviada a los expertos sea valorada por bloques, y no toda en su conjunto, de modo que pueda presentarse un consenso estadístico mucho más rápido, así es posible que pueda reducirse la cantidad de iteraciones del proceso.

Se recomienda para los auditores que recién comienzan el proceso de implementar un SGSI, no formen parte de la opinión de conceptos de la encuesta, de modo que surja efecto el objetivo principal el cual es reducir la subjetividad, ya que es posible que inicialmente sea una opinión muy influenciada por unas pocas experiencias en el campo.

Si bien el método Delphi según varios autores, recomienda una base de conocimiento entre 10 a 30 expertos, la idea es que la aplicación sea lanzada en el momento en el cual ya se cuenta con una base de conocimiento que se encuentre por encima de esta recomendación, para agregar más conocimiento en las opiniones.

6.3 Trabajo Futuro

Es posible que, dentro de las necesidades de cada organización, se realice una recomendación técnica a cada control de acuerdo al área en la que se aplica, como puede ser si el control indica que se debe asegurar el centro de procesamiento de datos para garantizar el ingreso de personal autorizado, entonces si es del caso, la aplicación podrá sugerir medidas técnicas para ellos, como son implementar control de acceso biométrico, tarjetas de proximidad, panel táctil, entre otros. Una de las falencias de estos estándares

es que no dicen el cómo debe hacerse, por lo que un valor agregado importante será comenzar con ese cómo.

Implementar en el prototipo la generación de reportes del estado de los controles usados, los controles evaluados, las personas involucradas en la organización con los riesgos asociados a un control en particular, y otros que puedan surgir de la necesidad de la organización.

Implementar como complemento de la aplicación un módulo de alertas tempranas que sugiera la revisión o reevaluación de controles por ciertos períodos de tiempo, actualización de controles por motivo de actualización en el estándar internacional, y cualquier otra gestión proactiva que pueda ser útil para el encargado del monitoreo del SGSI.

Consolidar la metodología como un insumo para las organizaciones, mediante la publicación en internet de la plataforma de modo que el trabajo colaborativo de los expertos pues llamar la atención de las organizaciones a unirse a la iniciativa y conseguir depurar y lograr una mayor robustez de todos los procesos involucrados en un eventual desarrollo del software.

Bibliografía

Acevedo, H. (2010). ITIL: ¿qué es y para qué sirve? Retrieved from http://www.magazcitum.com.mx/?p=50#.WDn0RbLhDak

Almenara, J. C., & Moro, A. I. (2014). Empleo del método Delphi y su empleo en la investigación en comunicación y educación. *Edutec, 48, 1-16*, 1–16. Retrieved from https://scholar.google.es/citations?view_op=view_citation&continue=/scholar%3Fhl%3Des%26as_sdt%3D0,5%26scilib%3D1&citilm=1&citation_for_view=33SfwF8AAAAJ:4hFrxpcac9AC&hl=es&oi=p

Arraj, V. (2013). ITIL ® : the basics. *Best Management Practice*, (July).

Beckers, K., Hofbauer, S., Quirchmayr, G., & Wills, C. (2013). A Method for Re-using Existing ITIL Processes for Creating an ISO 27001 ISMS Process Applied to a High Availability Video Conferencing Cloud Scenario. In A. Cuzzocrea, C. Kittl, D. Simos, E. Weippl, & L. Xu (Eds.), *Availability, Reliability, and Security in Information Systems and HCI SE - 16* (Vol. 8127, pp. 224–239). Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-642-40511-2_16

Blanco, C., Lasheras, J., Fernández-Medina, E., Valencia-García, R., & Toval, A. (2011). Basis for an integrated security ontology according to a systematic review of existing proposals. *Computer Standards and Interfaces*, *33*(4), 372–388. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-79953317215&partnerID=40&md5=f203d80a6d3a883d610753657ec43fd9

Boehmer, W. (2009). Cost-benefit trade-off analysis of an ISMS based on ISO 27001. *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 392–399. http://doi.org/10.1109/ARES.2009.128

Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, *11*(1), 26–31.

http://doi.org/http://dx.doi.org/10.1016/j.istr.2005.12.001

Cleave, M. Van. (2013). Edward Snowden , Bradley Manning and the Next Leak, 1–10.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297–334. http://doi.org/10.1007/BF02310555

De Sousa Pereira, R. F., & Da Silva, M. M. (2010). A maturity model for implementing ITIL v3. *Proceedings - 2010 6th World Congress on Services, Services-1 2010*, 399–406. http://doi.org/10.1109/SERVICES.2010.80

Deming, E. (1989). *Calidad, productividad y competitividad: la salida de la crisis*. (E. D. de Santos, Ed.). Madrid.

FIRST. (2015). Common Vulnerability Scoring System v3.0: Specification Document, 1–21. Retrieved from https://www.first.org/cvss/specification-document

Frías Navarro, D. (2014). Apuntes de SPSS, 3.

Fung, A. R.-W., Farn, K.-J., & Lin, A. C. (2003). Paper: A study on the certification of the information security management systems. *Computer Standards and Interfaces*, *25*(5), 447–461. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-0042468094&partnerID=40&md5=fc49fbc78fafc240f98484fbbfff5eb2

García, M., Quispe, C., & Ráez, L. (2003). Mejora continua de la calidad de los procesos. *Industrial Data*, *6*, 89–94.

Hajdarevic, K., & Allen, P. (2013). A new method for the identification of proactive information security management system metrics. *Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention on*, 1121–1126.

Iden, J., & Eikebrokk, T. R. (2013). Implementing IT Service Management: A systematic literature review. *International Journal of Information Management*, *33*(3), 512–523. http://doi.org/10.1016/j.ijinfomgt.2013.01.004

International Organization for Standardization. (2005a). ISO 27001:2005, Information technology - Security techniques. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en

International Organization for Standardization. ISO 27001:2005, Information technology - Security techniques — Information security management systems — Requirements (2005). Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en

International Organization for Standardization. (2013a). ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

International Organization for Standardization. (2013b). NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001, 37.

International Organization for Standardization. (2015). ISO Survey. Retrieved from http://www.iso.org/iso/iso-survey

ISACA. (2007). CoBIT 4.1. *IT Governance Institute*, 1–29. http://doi.org/10.1016/S0167-4048(97)84675-5

ISACA. (2012). *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*.

ISACA. (2016). COBIT 5 Foundation Exam. Retrieved from http://www.isaca.org/Education/COBIT-Education/Pages/COBIT-Exams.aspx

Iso 27001. (n.d.). Retrieved from http://www.iso27000.es/sgsi.html

Landeta, J. (1999). *El Método Delphi : una técnica de previsión para la incertidumbre*. (Ariel, Ed.). Barcelona : Ariel. Retrieved from http://www.fundacionmapfre.org/documentacion/publico/i18n/consulta/registro.cmd?id=19385

Mell, P., Scarfone, K., & Romanosky, S. (2007). A Complete Guide to the Common Vulnerability Scoring System Version 2.0. *FIRSTForum of Incident Response and Security Teams*, 1–23. Retrieved from http://www.first.org/cvss/cvss-guide.pdf

Nancylia, M., Mudjtabar, E. K., Sutikno, S., & Rosmansyah, Y. (2014). The Measurement Design of Information Security Management System. *IEEE Security and Privacy*, *10*(3), 200–205.

National Institute of Standards and Technology. (2011). Managing Information Security Risk. *NIST Special Publication 800-39*, (March). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

Neubauer, T., Ekelhart, A., & Fenz, S. (2008). Interactive Selection of ISO 27001 Controls under Multiple Objectives. In S. Jajodia, P. Samarati, & S. Cimato (Eds.), *Proceedings of The Ifip Tc 11 23rd International Information Security Conference SE - 31* (Vol. 278, pp. 477–492). Springer US. http://doi.org/10.1007/978-0-387-09699-5_31

OCDE. (2002). Directrices de la ocde para la seguridad de sistemas y redes de información, 1–12.

Paola, D., & Cadavid, B. (2011). *Modelo de correlación de las competencias del responsable de tecnología y el nivel de alineación estratégica de t.i.* Cali.

Pavlov, G., & Karakaneva, J. (2011). INFORMATION SECURITY MANAGEMENT SYSTEM IN ORGANIZATION, *9*(4), 20–25.

Peciña, K., Bilbao, A., & Bilbao, E. (2011). Physical and logical Security Risk Analysis

model. *Security Technology (ICCST), 2011 IEEE International Carnahan Conference on*, 1–7. http://doi.org/10.1109/CCST.2011.6095895

Pierce, B., & Sweeney, B. (2005). Management control in audit firms—Partners' perspectives. *Management Accounting Research*, *16*(3), 340–370. http://doi.org/10.1016/j.mar.2005.06.008

Ristov, S., & Kostoska, M. (2012). A New Methodology for Security Evaluation in Cloud Computing. *MIPRO, 2012 Proceedings of the 35th International Convention*, 1484–1489. Retrieved from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6240887&queryText=A+New+Methodology+for+Security+Evaluation+in+Cloud+Computing

Shojaie, B., Federrath, H., & Saberi, I. (2014). Evaluating the effectiveness of ISO 27001: 2013 based on annex A. *Proceedings - 9th International Conference on Availability, Reliability and Security, ARES 2014*, 259–264. http://doi.org/10.1109/ARES.2014.41

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards : A Comparative Study of the Big Five, (October).

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012). A Novel Method on ISO 27001 Reviews : ISMS Compliance Readiness Level Measurement, *2*(1), 1–12.

Talib, M. A., Khelifi, A., & Ugurlu, T. (2012). Using ISO 27001 in teaching information security. *IECON Proceedings (Industrial Electronics Conference)*, 3149–3153. http://doi.org/10.1109/IECON.2012.6389395

Tan, W.-G., Cater-Steel, A., & Toleman, M. (2009). IMPLEMENTING IT SERVICE MANAGEMENT: A CASE STUDY FOCUSSING ON CRITICAL SUCCESS FACTORS. *JOURNAL OF COMPUTER INFORMATION SYSTEMS*, *50*(2), 1–12.

Vanaclocha, P. (2009). Errores comunes en la Implantación de un SGSI. Retrieved from http://www.securityartwork.es/2009/03/29/errores-comunes-en-la-implantacion-de-

un-sgsi/

Villagrasa, R. (2015). El método Delphi y la toma de decisiones. *Apuntes: Revista de Ciencias Sociales*, *0*(5). Retrieved from http://revistas.up.edu.pe/index.php/apuntes/article/view/572

W. Edwards Deming, J. N. M. (1989). *Calidad, productividad y competitividad: la salida de la crisis*. (E. D. de Santos, Ed.).

Anexos

Perfiles de los expertos que participaron

- Experto 1, colombiano, Ingeniero de seguridad de la información Dann Regional, Magíster de Universidad Eafit, Colombia, 2 años de experiencia en seguridad de la información.

- Experto 2, colombiano, Auditor de Sistemas, Magíster de Universidad Nacional de Colombia, 3 años de experiencia en seguridad de la información.

- Experto 3, peruano, Oficial de seguridad de la información en SBN Perú, Especialista de Universidad Nacional del Nordeste, Argentina, 6 años de experiencia en seguridad de la información.

- Experto 4, colombiano, Lead Auditor de la compañía Bureau Veritas, Magíster de la Universidad de los Andes, 16 años de experiencia en seguridad de la información.

- Experto 5, colombiano, coordinador de sistemas, Especialista de Universidad del norte, 3 años de experiencia en seguridad de la información.

- Experto 6, chileno, Auditor de la compañía Entel Chile, Especialista de la Universidad Tecnológica Nacional de Chile, 10 años de experiencia en seguridad de la información.

- Experto 7, colombiano, Auditor de la compañía Coltefinanciera, Magíster de la Universidad Pontifica Bolivariana, 5 años de experiencia en seguridad de la información.

Encuesta enviada a expertos

FACTORES Y VARIABLES PARA SELECCIONAR CONTROLES CLAVES
¿LA OMISIÓN EN LA REALIZACIÓN DEL CONTROL PUEDE?
¿Afectar la integridad de los datos?
¿Afectar la disponibilidad de los datos?
¿Afectar la confidencialidad de los datos?
Afectar la efectividad de otros controles
¿EL IMPACTO O PÉRDIDA ECONÓMICA POR LA OMISIÓN DEL CONTROL PUEDE ASCENDER A?:

Ningún impacto económico
Pérdida económica inferior al 0,025% del Patrimonio Contable
Pérdida económica entre el 0,025% y el 0,15% del Patrimonio Contable
Pérdida económica entre el 0,15% y el 0,5% del Patrimonio Contable
Pérdida económica entre el 0,5% y el 1% del Patrimonio Contable
Pérdida económica superior al 1% del Patrimonio Contable
¿HISTORICAMENTE SE HAN PRESENTADO EVENTOS DE RIESGO POR LA OMISIÓN EN LA REALIZACIÓN DEL CONTROL?
Ningún evento de riesgo
Entre 1 y 5 eventos de riesgo
Entre 6 y 10 eventos de riesgo
Entre 11 y 20 eventos de riesgo
Más de 21 eventos de riesgo
¿EL IMPACTO O PÉRDIDA DE MERCADO POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:
Ningún impacto en el mercado
Incremento en los reclamos de algunos clientes.
Incremento en los reclamos de los clientes y/o posibilidad de pérdida de clientes.
Gran incremento en reclamos de clientes y /o alguna pérdida de estos.
Serias pérdidas de clientes.
Pérdida de clientes a gran escala.
¿EL IMPACTO REPUTACIONAL POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:
Ningún impacto reputacional
De conocimiento a nivel de la instalación y empresa.
De conocimiento a nivel local limitado.
De conocimiento a nivel regional.
De conocimiento a nivel nacional.
De conocimiento a nivel nacional e internacional.
¿EL IMPACTO EN EL CAPITAL HUMANO POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:
Ningún impacto en capital humano
Ausencia programada del personal no crítico.
Ausencia no programada del personal no crítico.
Ausencia programada del personal crítico u Ausencia definitiva del personal no crítico.
Ausencia no programada del personal crítico.
Ausencia definitiva del personal crítico.

¿EL IMPACTO EN LOS PROCESOS POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:
Ningún impacto en los procesos
Intermitencias o Interrupciones en la prestación del Servicio que requieren soluciones sencillas.
Interrupción temporal del Servicio, sin afectación de la infraestructura Física y/o tecnológica.
Interrupción temporal del servicio, con algunas dificultades para la recuperación de la infraestructura física y/o tecnológica.
Interrupción parcial del servicio e indisponibilidad de parte de la infraestructura física y/o tecnológica.
Interrupción total de la prestación del servicio e indisponibilidad de la infraestructura física y tecnológica.
¿LA POSIBILIDAD DE OCURRENCIA DE UN EVENTO OCASIONADO POR LA OMISIÓN DEL CONTROL ES?:
Ninguna posibilidad de ocurrencia
El evento puede ocurrir sólo bajo circunstancias excepcionales (Excepcionalmente)
Baja posibilidad de que el evento ocurra (Pocas Veces)
Existe una alta posibilidad de que el evento ocurra (Algunas Veces)
El evento ocurrirá en casi cualquier circunstancia (Varias Veces)
Se espera que el evento ocurra la mayoría de las circunstancias (Muchas Veces)

Tabla de calificación y resultados

FACTORES Y VARIABLES PARA SELECCIONAR CONTROLES CLAVES		
¿LA OMISIÓN EN LA REALIZACIÓN DEL CONTROL PUEDE?	**Respuesta**	**Peso de variable %**
¿Afectar la integridad de los datos?		33,33
¿Afectar la disponibilidad de los datos?	x	33,33
¿Afectar la confidencialidad de los datos?		33,33
¿EL IMPACTO O PÉRDIDA ECONÓMICA POR LA OMISIÓN DEL CONTROL PUEDE ASCENDER A?:	Elección	
Ningún impacto económico		0
Pérdida económica inferior al 0,025% del Patrimonio Contable		50%
Pérdida económica entre el 0,025% y el 0,15% del Patrimonio Contable		65%
Pérdida económica entre el 0,15% y el 0,5% del Patrimonio Contable		85%
Pérdida económica entre el 0,5% y el 1% del Patrimonio Contable	x	100%
¿HISTORICAMENTE SE HAN PRESENTADO EVENTOS DE RIESGO POR LA OMISIÓN EN LA REALIZACIÓN DEL CONTROL?		
Ningún evento de riesgo		0%
Entre 1 y 5 eventos de riesgo		50%
Entre 6 y 10 eventos de riesgo		65%
Entre 11 y 20 eventos de riesgo		90%
Más de 21 eventos de riesgo	x	100%
¿EL IMPACTO O PÉRDIDA DE MERCADO POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:		
Ningún impacto en el mercado		0%

Incremento en los reclamos de algunos clientes.		10%
Incremento en los reclamos de los clientes y/o posibilidad de pérdida de clientes.		60%
Gran incremento en reclamos de clientes y /o alguna pérdida de estos.		75%
Serias pérdidas de clientes.		90%
Pérdida de clientes a gran escala.	x	100%
¿EL IMPACTO REPUTACIONAL POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:		
Ningún impacto reputacional		0%
De conocimiento a nivel de la instalación y empresa.		40%
De conocimiento a nivel local limitado.		45%
De conocimiento a nivel regional.		65%
De conocimiento a nivel nacional.		95%
De conocimiento a nivel nacional e internacional.	x	100%
¿EL IMPACTO EN EL CAPITAL HUMANO POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:		
Ningún impacto en capital humano		0%
Ausencia programada del personal no crítico.		10%
Ausencia no programada del personal no crítico.		35%
Ausencia programada del personal crítico u Ausencia definitiva del personal no crítico.		55%
Ausencia no programada del personal crítico.		85%
Ausencia definitiva del personal crítico.	x	100%
¿EL IMPACTO EN LOS PROCESOS POR LA OMISIÓN DEL CONTROL PUEDE REPRESENTAR?:		
Ningún impacto en los procesos		0
Intermitencias o Interrupciones en la prestación del Servicio que requieren soluciones sencillas.		5%
Interrupción temporal del Servicio, sin afectación de la infraestructura Física y/o tecnológica.		10%

Interrupción temporal del servicio, con algunas dificultades para la recuperación de la infraestructura física y/o tecnológica.		30%
Interrupción parcial del servicio e indisponibilidad de parte de la infraestructura física y/o tecnológica.	x	65%
Interrupción total de la prestación del servicio e indisponibilidad de la infraestructura física y tecnológica.		100%
¿LA POSIBILIDAD DE OCURRENCIA DE UN EVENTO OCASIONADO POR LA OMISIÓN DEL CONTROL ES?:		
Ninguna posibilidad de ocurrencia		0%
El evento puede ocurrir sólo bajo circunstancias excepcionales (Excepcionalmente)		5%
Baja posibilidad de que el evento ocurra (Pocas Veces)		25%
Existe una alta posibilidad de que el evento ocurra (Algunas Veces)		55%
El evento ocurrirá en casi cualquier circunstancia (Varias Veces)		85%
Se espera que el evento ocurra la mayoría de las circunstancias (Muchas Veces)	x	100%

			Resultado	
Peso de variable porcentaje	**Peso de variable en puntos**	**Porcentaje calculado**	**Porcentaje del bloque para el control**	**Puntaje del bloque para el control**
10%	0,5	33%	3%	**0,16665**
20%	1	100%	20%	**1**

10%	0,5	100%	10%	**0,5**
10%	0,5	100%	10%	**0,5**
10%	0,5	100%	10%	**0,5**
20%	1	100%	20%	**1**

10%	0,5	65%	7%	**0,325**
10%	0,5	100%	10%	**0,5**

Puntaje para el control	**4,49**