Implantación de la fase Ejecución de un SGSI[1] adaptando un marco de referencia con base en la norma ISO/IEC 27001:2013.

Fabio Hernán Cerón Calvo
Deisy Francely Imbachi Arboleda

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Grupo de Tecnologías de la Información (GTI)
Línea de Investigación: Seguridad Informática
Popayán, Octubre de 2017

[1] Sistema de Gestión de Seguridad de la Información.

Implantación de la fase Ejecución de un SGSI adaptando un marco de referencia con base en la norma ISO/IEC 27001:2013.

Trabajo de Grado presentado como requisito para obtener el título de Ingeniero en Electrónica y Telecomunicaciones y al título de Ingeniero de sistemas

Fabio Hernán Cerón Calvo
Deisy Francely Imbachi Arboleda

Director: Mg. Siler Amador Donado

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Grupo de Tecnologías de la Información (GTI)
Línea de Investigación: Seguridad Informática
Popayán, Octubre de 2017

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

Director:

_____
Siler Amador Donado

_____
Firma Jurado

_____
Firma Jurado

Fecha:

AGRADECIMIENTOS

Agradecimientos

A nuestros padres quienes, con su amor incondicional y dedicación acompañaron e impulsaron nuestro proceso formación.

A nuestras familias quienes con paciencia y comprensión fueron el apoyo que nos permitió levantarnos con más fuerza y motivación luego de cada tropiezo.

A nuestro director Mg Siler Amador Donado quien con sus conocimientos y experiencia supo guiarnos en todo momento.

A Dokia Marisol Zúñiga Mosquera, jefe de la División de admisiones, registro, y control académico DARCA, quien permitió llevar a cabo este trabajo de grado.

Finalmente, a nuestra alma mater la Universidad del Cauca, por abrirnos sus puertas, acogernos, formarnos y permitirnos alcanzar este anhelado logro.

A todos ellos, muchas gracias.

RESUMEN

Este proyecto de investigación propone la adaptación de un marco de referencia que cumple con los requisitos de la norma ISO / IEC 27001: 2013 y que incluye los componentes del Modelo EFQM. El propósito del marco de referencia es realizar la implantación de la fase de *Ejecución* de un SGSI (Sistema de Gestión de Seguridad de la Información) en el procedimiento *Inscripciones y Admisiones*, para el alcance de DARCA (División de Admisiones, Registro y Control Académico) de la Universidad del Cauca.

La implementación de un SGSI sigue el enfoque del ciclo Deming o ciclo de mejora continua PHVA (Planear-Hacer-Verificar-Actuar). La fase *Ejecución* es la segunda fase del ciclo Deming, y depende de la fase *Planear*. Por lo tanto, fue necesario examinar y replantear la fase *Planear* del SGSI para el procedimiento *Inscripciones y Admisiones*.

Este proyecto se realizó en dos pasos. El primer paso fue la definición de los lineamientos que se deben seguir para para armonizar el modelo EFQM y la norma ISO/IEC 27001. Posteriormente, se realizó la adaptación siguiendo los lineamientos encontrados a fin de plantear un marco de referencia. El segundo paso fue desarrollar la fase de *Ejecución* de un SGSI en el procedimiento *Inscripciones y Admisiones* con el marco de referencia propuesto.

ABSTRACT

This research project proposes the adaptation of a framework that meets the requirements of ISO / IEC 27001: 2013 and includes the components of the EFQM Model. The purpose of framework is the implementation of *Do* phase of ISMS (Information Security Management System), in the *Registration and Admissions* procedure, for the scope of DARCA (*Division of Admissions, Registration and Control Academic)* of the University of Cauca.

The implementation of an ISMS follows the Deming cycle or continuous improvement cycle PDCA (Plan-Do-Check-Act). The *Do* phase is the second phase of the Deming cycle, and depends on the *Plan* phase. Therefore, it was necessary to examine and rethink the process of the *Plan* phase of ISMS for the *Inscriptions and Admissions* procedure

This project was carried out in two steps. The first step was the definition of the guidelines that should be followed to harmonize EFQM model and ISO/IEC 27001 standard. Subsequently, the adaptation was made following the guidelines found in order to propose a framework. The second step was developing the *Do* phase of ISMS in the *Inscriptions and Admissions* procedure, whit the proposed framework.

TABLA DE CONTENIDO

ANEXOS

INDICE DE FIGURAS

INDICE DE TABLAS

1. CAPITULO I. INTRODUCCIÓN

1.1. PLANTEANIENTO DEL PROBLEMA

1.1.1. Definición

La seguridad de la información es clave para las organizaciones que buscan reducir los riesgos de los sistemas de información a un nivel aceptable [1], [2]. Para que esto sea posible es preciso realizar un trabajo articulado entre el gobierno y las empresas. El gobierno Colombiano por su parte, ha realizado esfuerzos en materia de seguridad de la información [3], [4], sin embargo la mayoría de las empresas en Colombia no poseen planes de respuesta frente a incidentes de seguridad informática [5], [6]. Es por ello que se evidencia la importancia de implantar un adecuado SGSI (Sistema de Gestión de la Seguridad de la Información) en las organizaciones de Colombia con el fin de identificar y reducir los riesgos de los activos de información. En este contexto se considera particularmente la necesidad de implantación de un SGSI en las universidades públicas de Colombia.

Para llevar a cabo la implantación de un SGSI es indispensable utilizar la norma internacional ISO/IEC 27001[7], dado que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI. Además, la certificación de un SGSI se realiza de conformidad con la norma ISO/IEC 27001, sin embargo, esta norma es de carácter universal aplicable a organizaciones de cualquier sector y actividad productiva, sin tener en cuenta los costos de su aplicación, ni las particularidades que tienen las universidades públicas de Colombia. El conjunto de normas ISO/IEC 27000 [8], ISO/IEC 27002 [9], ISO/IEC 27003 [10], ISO/IEC 27004 [11] e ISO/IEC 27005 [12] se limitan a establecer una serie de recomendaciones generales para apoyar la implantación de un SGSI, y a pesar de ser muy útiles, no son suficientes cuando se trata de responder a las necesidades propias de las universidades públicas de Colombia.

La norma ISO/IEC 27001 presenta un sistema de gestión basado en el ciclo de Deming [13] que contempla las etapas Plan, Do, Check, Act (Planear, Hacer, Verificar, Actuar) y estas se llevan a cabo en orden secuencial. Así pues, este trabajo de grado está enfocado específicamente en la fase Do (Hacer) o fase *Ejecución* del SGSI. Además, debido a la complejidad de las universidades se selecciona un solo departamento, para este caso el *Departamento de Registro y Control Académico – DARCA* de la Universidad del Cauca. Teniendo en cuenta estas consideraciones, se toman como punto de partida los resultados obtenidos y presentados en [14], que

corresponden a la realización de la fase plan en el procedimiento "*Inscripciones y Admisiones*" de División de Admisiones, Registro y Control Académico - DARCA de la Universidad del Cauca.

La norma ISO/IEC 27001 establece *qué* requisitos debe cumplir un SGSI, sin embargo, la norma no tiene una especificación concreta respecto a prácticas o procesos de calidad para un SGSI. En este sentido, la norma ISO/IEC 27001:2013 no establece directrices en relación a la calidad y mejoramiento de procesos con respecto a un SGSI. Existe una amplia gama de modelos y estándares internacionalmente reconocidos que se enfocan en la calidad y mejoramiento de procesos, p.ej. CMM, CMMI, ISO 9001, ISO 20000, ISO 90003, sólo para nombrar algunos. También están los modelos de gestión de la calidad Malcolm Baldrige, Modelo EFQM y el modelo Iberoamericano.

De los modelos y estándares enfocados en calidad, se seleccionó el modelo EFQM por su adaptabilidad y principalmente por su enfoque de autoevaluación continuo que permite estimular el mejoramiento continuo de un SGSI. El esquema de autoevaluación que brinda el modelo EFQM permite establecer y evidenciar un mejoramiento permanente del SGSI que sirve de apoyo hacia la certificación de la norma ISO/IEC 27001. De esta manera se plantea el problema de establecer el SGSI, específicamente la fase *Ejecución* del SGSI en el procedimiento Inscripciones y Admisiones, perteneciente a DARCA de la Universidad del Cauca, de conformidad con la norma ISO/IEC 27001, a la vez que se agregan elementos de calidad proporcionados por el modelo EFQM.

Finalmente, en el presente trabajo de grado se plantea la necesidad de adaptar un marco de referencia a la fase ejecución de un SGSI siguiendo los requisitos de la norma ISO/IEC 27001 y haciendo uso del modelo EFQM, el cual se emplea en un departamento de registro y control académico de una institución pública universitaria.

1.1.2. Pregunta de Investigación

Considerando la definición del problema se propone la siguiente pregunta a la cual se le dará respuesta a lo largo del desarrollo del presente proyecto:

¿Cómo adaptar un marco de referencia usando el modelo EFQM y la norma ISO/IEC 27001 para la implantación de la fase ejecución de un SGSI en un departamento de registro y control académico de una institución pública universitaria?

1.1.3. Justificación

La seguridad de la información ha sido un tema que ha cobrado mayor importancia en los últimos años debido a los incidentes de seguridad de gran envergadura que suceden al interior de las Universidades públicas de Colombia, por eso ha surgido un gran interés de nuestra parte para abarcar este tema con el propósito de adquirir conocimientos normativos, metodológicos y prácticos que se puedan utilizar en beneficio de las universidades públicas de Colombia y especialmente de la División de Admisiones, Registro y Control Académico – DARCA de la Universidad del Cauca.

Como ya se ha dicho anteriormente es innegable la necesidad de implantar un SGSI en las Universidades Publicas, con lo cual se sustenta la necesidad de realizar este proyecto. Además, al revisar los antecedentes, se encontró que actualmente muchas organizaciones de todo el mundo cuentan con la necesidad de establecer soluciones prácticas de integración, unificación, adaptación, alineación o armonización de diversos modelos y/o estándares; y una de las organizaciones es la Universidad del Cauca. Adicionalmente, se encontró que a la fecha no se ha realizado una adaptación entre la norma ISO/IEC 27001:2013 y el modelo EFQM: 2013.

Se han desarrollado proyectos que buscan utilizar las mejores características de los marcos de referencia para aprovecharlos en beneficio de las organizaciones, sin embargo, el elemento diferenciador de este proyecto es el Modelo EFQM en beneficio de una futura certificación de la norma ISO/IEC 27001:2013 en el departamento de Registro y Control Académico de la Universidad del Cauca.

Esta investigación tiene aportes divididos en dos componentes, un componente de innovación y un componente de desarrollo. El primero se centra en realizar una adaptación de un marco de referencia específico para la fase *Ejecución* de un SGSI siguiendo la norma ISO/IEC 27001 y el modelo EFQM, para un departamento de Registro y Control Académico en una institución pública universitaria de Colombia; mientras que el componente de desarrollo se enfoca en utilizar el marco de referencia obtenido, en el procedimiento *Inscripciones y Admisiones* de DARCA de la Universidad del Cauca.

Este proyecto sirve de guía para que los procesos y/o procedimientos críticos de la Universidad del Cauca, y de otras Universidades públicas que ya hayan desarrollado la fase *Plan* del SGSI según el modelo PHVA, puedan continuar con la fase *Ejecución* del SGSI. Además se destaca que este proyecto es un aporte de gran

relevancia para el proyecto titulado “Sistema de Gestión de la Seguridad de la Información de la Universidad del Cauca” [15].

Este proyecto especifica una serie de recomendaciones para realizar la fase *Ejecución* del SGSI cumpliendo los requisitos de la norma ISO/IEC 27001, aprovechando también los componentes de calidad que brinda en modelo EFQM. Finalmente, se recomienda integrar la norma ISO/IEC 27001 con otros sistemas de gestión normalizados como ISO 9001, e ISO 14001 para obtener resultados perdurables en el tiempo.

1.2. OBJETIVOS DE LA INVESTIGACIÓN

1.2.1. Objetivo general

Adaptar un marco de referencia[2], usando el modelo EFQM y los requerimientos de la norma ISO/IEC 27001, para implantar la fase *Ejecución* de un SGSI en el procedimiento “Inscripciones y Admisiones” de DARCA de la Universidad del Cauca

1.2.2. Objetivos específicos

- ✓ Definir los lineamientos[3] para adaptar un marco de referencia a la fase ejecución de un SGSI, según el modelo EFQM y los requerimientos de la norma ISO/IEC 27001.
- ✓ Adaptar un marco de referencia a la fase de ejecución de un SGSI siguiendo los lineamientos encontrados.
- ✓ Implantar la fase ejecución de un SGSI utilizando el marco de referencia adaptado en el procedimiento “Inscripciones y Admisiones” de DARCA de la Universidad del Cauca.

[2] Marco de Referencia: Concepto de noción general que abarca modelos, metodologías, normas, estándares, guías, prácticas y/o una adaptación de ellas

[3] Lineamientos: Dirección, Tendencia, Rasgo Característico de algo. (Definición RAE)

1.3. ESTRATEGIA DE INVESTIGACIÓN

La estrategia empleada para el desarrollo de este trabajo de grado se basa en el método de investigación cualitativo investigación-acción (IA). Dada la variedad en definiciones de IA se toma la postura de [16], citado en [17] (p.63) en donde la investigación-acción "*consiste en la participación de todos los miembros de la investigación en el estudio del escenario problemático actual, en un esfuerzo por mejorarlo o cambiarlo"*.

Según [18], citado en [17] (p.68) existen variaciones en la forma que se aplican los *productos de investigación*[4] sobre el *grupo crítico de referencia*[5]. En este sentido, esta investigación corresponde a una investigación-acción de tipo "**colaboración**" en donde "*el grupo de referencia crítico pone en marcha las recomendaciones hechas por el investigador, e informa de los efectos*".

La Fig. 1 muestra el proceso aplicación de la IA empleado en este proyecto de investigación. Este proceso se basa en lo propuesto por [17] (p.65), y consta de tres fases: una primera fase de "Ciclo de investigación", una segunda fase de "Producto de investigación" y finalmente una tercera fase de "Ciclo de solución del problema".

Fig. 1. Proceso de investigación para la aplicación de investigación-acción. [17] (p.65). Fuente modificada

[4] Productos de investigación: Son los productos de trabajo generados durante el proceso de investigación que abordan tanto el tema de la investigación como el problema a resolver [17].

[5] Grupo crítico de referencia: Un grupo en el que se realiza la investigación, en vista de que tiene un problema que necesita ser resuelto. En este grupo hay personas que participan en la investigación, y pueden participar en el proceso de investigación, aunque no tan activamente como el investigador [17].

1.3.1. Fase 1. Ciclo de Investigación[6].

1.3.1.1. Metodología de investigación

La metodología utilizada para el desarrollo del *Ciclo de investigación* se basa en la "Metodología de la Investigación. Diseño y Ejecución" propuesta por V. M. Niño Rojas [19]. En éste se plantean las tres etapas que se muestra en la Fig. 2. Adicionalmente para efectos del presente trabajo de grado se adicionó una etapa transversal llamada *"Documentación"*.

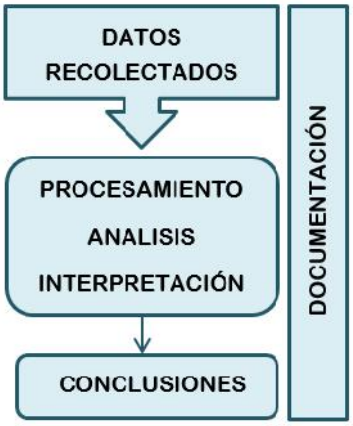

Fig. 2. Etapas para el desarrollo del proyecto. [19] (p.99)
Fuente Modificada

- ✓ **Datos Recolectados:** La recolección de los datos se realiza mediante el diseño y aplicación de las técnicas e instrumentos de recolección de datos.
- ✓ **Procesamiento, Análisis e Interpretación:** El procesamiento de los datos consiste en darle sentido a los datos recolectados generando unos resultados que definen el curso de la investigación.
- ✓ **Conclusiones:** Es la capacidad que tiene el investigador de dar a conocer las experiencias vividas durante el desarrollo de la investigación, y destacar los resultados más valiosos de la investigación.
- ✓ **Documentación:** La documentación constituye un registro del proceso de investigación en la monografía.

---

[6] Ciclo de investigación: Comprende el desarrollo de actividades que conllevan a definir el enfoque de la IA. Este enfoque se basa en una visión integrada de las áreas de interés y en el problema que necesita ser resuelto

1.3.1.2. Aplicación de la metodología de la investigación

La Tabla I ilustra las actividades que hacen parte del *ciclo de investigación,* y que se llevaron a cabo empleando la metodología propuesta por V. M. Niño.

TABLA I. Actividades para aplicación de la Metodología de investigación.

Etapa de la Metodología	Búsqueda Bibliográfica	Procedimiento Inscripciones y Admisiones
Datos Recolectados	– Recolección de unidades documentales referentes a la norma ISO/IEC 27001, modelo EFQM y marcos de referencia diversos. – Selección de unidades documentales – Registro de las unidades documentales	– Elaboración de los instrumentos – Aplicación de las técnicas de recolección de datos – Registro de la información
Procesamiento, análisis e interpretación	– Organización de unidades documentales – Clasificación de unidades documentales – Codificación de unidades documentales – Tabulación de unidades documentales – Análisis de unidades documentales – Interpretación de unidades documentales	– Organización de los datos – Clasificación de los datos – Codificación de los datos – Tabulación de los datos – Análisis de los datos – Interpretación de los datos
	Análisis de resultados Interpretación de resultados	
Conclusiones	Planteamiento de los lineamientos de un marco de referencia con base en los resultados	

1.3.2. Fase 2. Producto de Investigación

Comprende las siguientes actividades:

- Recolección de información requerida para dar cumplimiento a los lineamientos encontrados
- Selección de información
- Adaptación de un marco de referencia para la fase *Ejecución* de un SGSI
- Verificación del Cumplimiento de los lineamientos.

1.3.3. Fase 3. Solución de problemas

Comprende las siguientes actividades:

- Recolección y procesamiento de información requerida por el marco de referencia.
- Recolección de datos para determinar el estado inicial de la seguridad de la información
- Procesamiento de datos para determinar el estado inicial de la seguridad de la información.
- Establecimiento del estado inicial de la seguridad de la información
- **Implementación del SGSI en el procedimiento *Inscripciones y Admisiones.***
- Recolección de datos para determinar el estado final de la seguridad de la información.
- Procesamiento de datos para determinar el estado inicial de la seguridad de la información.
- Establecimiento del estado inicial de la seguridad de la información
- Identificación de aspectos positivos, negativos y aspectos críticos del proceso de implementación del SGSI (Redacción de un reporte de experiencias)

1.4. LIMITACIONES DE LA INVESTIGACIÓN

- Falta de expertos que apoyen el desarrollo de SGSI
- Falta de una certificación en la norma ISO/IEC 27001, y EFQM por parte de los investigadores
- Falta de disponibilidad del personal de DARCA de la Universidad del Cauca.
- Limitaciones de tipo tiempo, ya que ésta investigación se encuentra para un total de 36 semanas, siendo un tiempo muy corto para poder evidenciar los verdaderos efectos de este trabajo de grado.

1.5. ESTRUCTURA DEL DOCUMENTO

Capítulo 2. Se describen los fundamentos necesarios para entender y abordar la adaptación entre la norma ISO/IEC 27001:2013 y el modelo EFQM:2013. Se realiza una contextualización del procedimiento inscripciones y Admisiones, luego, se describen las dos primeras fases del ciclo Deming para un SGSI y el modelo de armonización seleccionado.

Capítulo 3. Se aborda la descripción de la armonización realizada entre la norma ISO/IEC 27001:2013 y el modelo EFQM:2013, con lo cual se estableció un marco de referencia para implementar la fase *Ejecución* del SGSI.

Capítulo 4. Contiene las conclusiones, aportes, recomendaciones y trabajos futuros en relación con este trabajo de grado.

2. CAPITULO II. FUNDAMENTOS

Para comenzar se realiza una descripción de las razones que han llevado a seleccionar el modelo EFQM como el elemento de innovación para ser adaptado con la norma ISO/IEC 27001. Luego se presenta los antecedentes acerca de algunos modelos que proporcionan soluciones para realizar la adaptación de diferentes marcos de referencia, logrando finalmente la selección uno de ellos.

Después, se contextualiza el procedimiento *Inscripciones y Admisiones* de DARCA de la Universidad del Cauca, siendo éste el enfoque de acción de este trabajo de grado. Finalmente se presenta el marco teórico en donde se describe de manera general el modelo de adaptación seleccionado, la norma ISO/IEC 27001:2013, el ciclo Deming, la fase *Plan* del SGSI, la fase *Ejecución* del SGSI y el modelo EFQM:2013. Todo esto con el propósito de tener una mayor comprensión de los elementos que componen este trabajo de grado.

2.1. ANTECEDENTES

2.1.1. Modelos y estándares de Calidad

Un SGSI se implementa y certifica dando cumplimiento a los requisitos especificados en la norma ISO/IEC 27001: 2013, pese a ello, es necesario agregar elementos que permitan alcanzar un SGSI de calidad. Ahora bien, la razón por la cual se adoptan prácticas de calidad son principalmente la *satisfacción del cliente, la disminución de los fallas y la adquisición de competencias* [20] (pp.12-13).

Existen múltiples modelos y estándares de calidad, que se dividen según su enfoque a nivel de producto y a nivel de servicio [21] (pp. 43-247). Entre los marcos de referencia más destacados se encuentran CMM, CMMI, SPICE e ISO 9001 [22] (p.39), siendo el estándar ISO 9001 uno de los más utilizados y reconocidos Internacionalmente. Este reconocimiento se debe a que el estándar ISO 9001 fue creado para establecer un nivel mínimo y uniforme de calidad, de manera que las organizaciones pudieran competir en igualdad de condiciones en un comercio internacional [23] (p.10). La aplicación de CMMI es una norma dirigida a grandes empresas que tienen requisitos de calidad muy altos, implicando elevados costos.

Sin embargo, las críticas sobre la familia de normas ISO 9000 está dada por la burocracia que genera en las empresas, es decir que los requisitos documentales son muy extensos [24], convirtiéndose en algo tedioso cuando la documentación no general algún valor para la organización. En este orden de ideas, la certificación se

basa en el estricto cumplimiento de las clausulas, las cuales en su mayoría corresponden a ***documentación*** de: los procesos operativos, del sistema de control y de las actividades de apoyo [23] (ver Tabla II). Para terminar, las criticas están dadas porque la norma ISO 9001 mira sólo al interior de la organización [25] (p.105). Aunque la norma es muy buena, no considera los resultados de la empresa, los logros de la misma en satisfacción a sus clientes, en proyección en la sociedad o en las perspectivas de viabilidad del negocio [25].

Este es el momento donde entran en juego los modelos de gestión de Calidad Total, entre los que se tienen: modelo EFQM, modelo Iberoamericano, y modelo Malcolm Baldrige. Todos ellos hacen hincapié en los resultados hacia los clientes, empleados, sociedad, y todos aquellos que pueden significar un riesgo para la organización [23] (p.2). La Tabla II muestra que cada uno de los modelos en mención va mucho más allá de la estricta documentación. En [26] se realiza un estudio comparativo entre los modelos más desarrollados a nivel conceptual, y aplicados por las empresas (Malcolm Baldrige, el Deming y EFQM), obteniendo que las empresas que han ganado premios basados en el modelo EFQM han conseguido incrementar su rentabilidad al año siguiente de ganarlo. El modelo iberoamericano por su parte es muy similar al modelo EFQM, pero tiene poca capacidad de actualización.

Según [27] y [28] publicados en años recientes indican que para lograr excelentes resultados en la implementación de la gestión de la calidad en un entorno empresarial real es indispensable emplear el modelo EFQM.

Una de las características que distingue al modelo EFQM frente a las normas ISO es que las organizaciones se evalúan a sí mismas basándose de esta manera en la autoevaluación, y no en la evaluación externa. Adicionalmente, la evaluación del modelo EFQM en caso de querer obtener un sello de excelencia[7], se enfoca un 55% en las personas y un 45% en la dirección y los mandos [29], mientras que las normas ISO que se enfocan un 70% en la Dirección y los mandos.

Teniendo en cuenta que el modelo EFQM describe un esquema de autoevaluación basado en la mejora continua empleando el esquema lógico REDER, cada iteración realizada establece las bases para la toma de acciones, que permiten evaluar el

[7] Sello de excelencia: Reconocimiento al uso del modelo EFQM, lo cual quiere decir que las organizaciones que llevan a cabo principios de la administración de la calidad total.

progreso hacia el cumplimiento del modelo, y con ello un evaluar el avance hacia la excelencia.

TABLA II. Modelos de Calidad. [23] (pp. 9-10)

	Premio Baldrige	Premio Europeo de calidad EFQM	Premio Iberoamericano	Certificación ISO 9000
Año de creación	1987	1992	1999	1987
Estructura básica	Concurso anual	Concurso Anual	Concurso Anual	Certificación
Enfoque	Liderazgo del cliente; apoyo a la organización; medición; benchmarking	Facilitadores de la organización y resultados; liderazgo, procesos y resultados.	Facilitadores de la organización y resultados; liderazgo, clientes y resultados.	Estándares mínimos de calidad global igualitarios; documentación del sistema de control, de los procesos operativos y actividades de apoyo.
Coste	Medio-alto	Medio-alto	Medio-alto	Bajo-medio

En los últimos años el modelo EFQM surgió como un modelo de gestión de calidad con perspectiva integradora, más amplia que el modelo definido en las normas ISO 9000 [25]. El modelo EFQM visto como un modelo para un Sistema Integrado de Gestión – SIG, en ingles IMS, tiene un enfoque global y completo. Ahora el modelo EFQM se encuentra en concordancia y/o compatibilidad con las múltiples normas ISO, entre las que se tiene: la norma ISO/IEC 9001 [30], ISO/IEC 27001, ISO/IEC 14001, ISO/IEC 20000 [31] solo por mencionar algunas. Este conjunto de normas ISO tienen elementos comunes que encajan dentro del modelo EFQM. Es preciso destacar que en [30] los resultados muestran que EFQM implica un avance sobre ISO 9000 en relación con el uso de prácticas de trabajo innovadoras. El modelo EFQM establece nueve criterios, los primeros cinco (Criterios Agentes) definen un sistema de gestión comparable con las normas ISO, mientas que los otros cuatro criterios (Criterios Resultados) permite avanzar en un área que las normas citan brevemente [25] (p.110).

El modelo EFQM tiene una opinión positiva en cuanto a modelo teórico y paradigma de gestión [32] (pp.134-135), produciendo mejores resultados que otros sistemas de calidad en los siguientes ámbitos:

· Mejora de la imagen externa: reputación, reconocimiento público.

· Clima laboral, satisfacción, motivación e implicación del personal.

· Competitividad: diferenciación con respecto a la competencia.

· Cultura y valores de la organización.

· Dinámica de Mejora Continua.

Según Navarro F., *El objetivo final de la aplicación del Modelo EFQM, es* ***aumentar la eficacia y eficiencia*** *de las organizaciones europeas, mediante* ***el refuerzo de la Calidad,*** *en todos los aspectos posibles de todas sus actividades****,*** *a la vez, que se desarrolla una dinámica de* ***mejora continua de la Calidad*** *dentro de las propias organizaciones* [33], propósito que, para el presente proyecto de investigación se orienta hacia el SGSI de conformidad con la norma ISO/IEC 27001:2013.

Finalmente, este trabajo de grado plantea la necesidad de armonizar la norma ISO/IEC 27001:2013 con el modelo EFQM:2013. En este orden de ideas, es preciso aclarar que la adaptación que se propone, toma como eje principal a la norma ISO/IEC 27001, en aras de beneficiar una futura certificación del SGSI.

2.1.2. Modelos que soportan una armonización

Existen gran variedad de proyectos relacionados con la integración, adaptación, unificación, alineación, combinación o fusión de marcos de referencia. Algunos de ellos son [34], [35], [36], [37], [38], [39], [40]. Gran cantidad de investigadores y organizaciones han tenido la necesidad de armonizar normas, metodologías, estándares, guías, prácticas y otros. Además, la necesidad de armonizar varios marcos de referencia depende de las características de cada organización [41], y actualmente sigue siendo de alta importancia para las empresas [42], [43], [44], [45].

A nivel nacional se ha trabajado en la armonización e implementación de marcos de referencia como ITIL, COBIT y la ISO 20000-27000 [46]; ISO 20000 e ISO 27001 [47], [48]; ISO 9001-2008 y EFQM [49], entre otros. Por su parte la Universidad del Cauca ha venido trabajando en la adaptación de algunos marcos de referencia con un enfoque hacia la seguridad de la información, es decir una adaptación entre OCTAVE-S y la norma ISO/IEC 27005:2011 [14]; entre NIST- SP 800-30 y la norma ISO/IEC 27005:2011 [50]; entre MAGERIT V3 y la norma ISO/IEC 27005:2011 [51], y otros en desarrollo actualmente. Es preciso resaltar que los trabajos mencionados, realizados en la Universidad del Cauca se encuentran enmarcados dentro de un proyecto macro titulado “Implantación y Certificación del Sistema de Gestión de la Seguridad de la Información de la Universidad del Cauca” [15].

Para realizar una armonización entre dos o más marcos de referencia no es suficiente con realizar una comparación, debido a las diferencias estructurales que

pueden existir entre ellos. Por lo tanto, es necesario definir un *modelo o técnica*[8] general que permita realizar dicha adaptación. Un modelo básicamente permitiría realizar una armonización entre múltiples marcos de referencia, empleando una escala de comparación que minimice la subjetividad.

Frente a la necesidad de armonización de estándares y modelos han surgido diferentes propuestas, entre las cuales se tienen:

- *Kelemen - Una unificación basada en procesos de enfoques de calidad de software orientados a procesos:* Realiza un resumen de las soluciones referentes a problemas multimodelos y propone un método para la unificación basada en procesos de múltiples enfoques de calidad de software. [52]

- *PrIME - The Process Improvement in Multimodel Environments:* Proyecto asesorado por SEI (Software Engineering Institute). Propone el mejoramiento de procesos en entornos multimodelos, abarcando gran variedad de temas relacionados con modelos ampliamente utilizados en la industria como Six Sigma, CMMI, Lean y Agile [53].

- *Ferchichi:* Propone un modelo de referencia para la interoperabilidad entre los procesos de las organizaciones de software. La solución propone cuatro pasos: Modelos de elección, Análisis de la sinergia de los modelos, La construcción de un modelo integrado, y finamente la adaptación del modelo integrado [54].

- *IDEAL model:* Este modelo fue asesorado por el Instituto de Ingeniería del Software. El modelo propone una guía para desarrollar un plan integrado de largo alcance con el propósito de iniciar y administrar un programa SPI [55].

- *IMPACT Project:* Presenta un marco de trabajo para SPI. Este marco ha sido diseñado para emplear una amplia gama de tecnologías para beneficiar los procesos existentes en las PYMEs. El marco se diseñó para ser aplicado de manera continua a fin de mejorar tiempo y costos en los proyectos. [56]**.**

- *Un enfoque de mejora de procesos de 360 grados basado en múltiples modelos:* Propone un marco de trabajo que define los elementos necesarios

[8]Un modelo o una Técnica proporcionan una serie de pasos ordenados para combinar varios marcos de referencia.

para apoyar la armonización de modelos y estándares de aplicabilidad en las organizaciones [57].

Sin embargo, se destaca el trabajo realizado por el investigador César Pardo en dirección y codirección de Félix García, Francisco Pino, Mario Piattini y M. Teresa Baldassarre, por cuanto se han realizado un conjunto de trabajos enfocados en la definición de soluciones relacionadas con los modelos de integración o unificación [58], [59], [60], [61], los cuales llevaron a proponer en el año 2011 un "*Modelo de integración para soportar la armonización de múltiples modelos y estándares*" [62]. Finalmente, en la búsqueda de la armonización de modelos múltiples, se propuso un marco de referencia denominado *HFramework* [22], el cual define tres componentes que apoyan la armonización de múltiples modelos y estándares. Posteriormente, la propuesta obtenida se ilustra en dos estudios de caso [63], El primero de ellos se llevó a cabo para organización de España, realizando una armonización entre ISO 27001 e ISO 20000-2 [64]; el segundo estudio de caso fue realizado para organización del sector bancario de Guatemala, realizando una armonización entre COBIT 4.1, Basel II, Val IT, Risk IT, ISO 27002 e ITIL V3.

Adicionalmente HFramework fue empleado para un Spinoff de Italia, realizando un análisis de relaciones entre la familia ISO como ISO 9001: 2008, ISO 27001: 2005 e ISO 20000-2: 2011, y su relación con CMMI-DEV V1.3 [22]. Finalmente se resalta la aplicabilidad de HFramework en diferentes entornos empresariales de gran importancia, por ejemplo, aplicado en la armonización entre COBIT 5, ISO 20000-2, CMMI- DEV, ISO 29110 [65].

Finalmente, es importante enfatizar en el extenso y excelente trabajo sintetizado en HFramework [22], el cual cuenta con una trayectoria de aplicación en proyectos a nivel nacional e internacional donde se han obtenido resultados satisfactorios. Esta propuesta establece los elementos necesarios para poner en consonancia diversos modelos y estándares de poca similitud y es una excelente opción para realizar la adaptación entre la norma ISO/IEC 27001 y el modelo EFQM.

En este orden de ideas, este trabajo de grado emplea los dos primeros componentes de HFramework, es decir, el marco Conceptual [60] y el marco metodológico [62], debido a que estos componentes han sido validados en diversos contextos organizacionales.

2.2. ESTRUCTURA DE PROCESOS Y PROCEDIMIENTOS DE LA UNIVERSIDAD DEL CAUCA

La Universidad del Cauca es una organización muy grande y compleja que emplea un modelo de operación por procesos, como una herramienta para examinar la dinámica de la Institución a partir de la identificación de los procesos y sus interacciones. La Universidad del Cauca ha agrupado los procesos afines en Macro procesos. Dependiendo del tamaño y la complejidad de algunos procesos, estos se descomponen en subprocesos. Luego, los subprocesos se llevan a cabo por medio de procedimientos [66]. Finalmente, los procedimientos se componen de actividades, tal como se muestra en la Fig. 3.

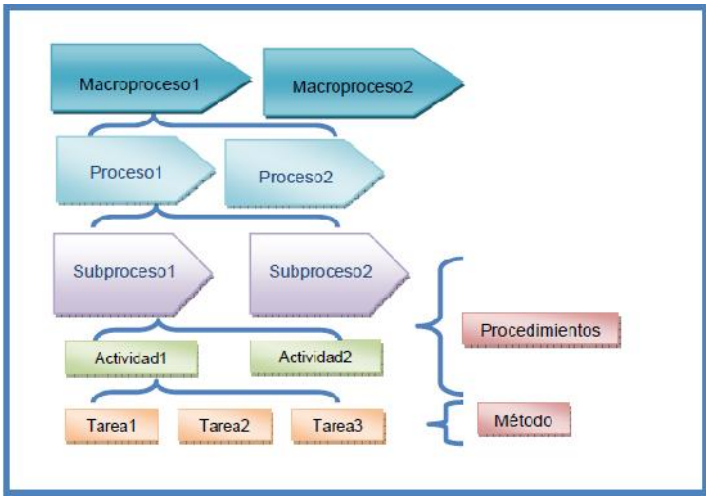

Fig. 3. Despliegue del Modelo de operación por procesos. [66]

En este orden de ideas, según el mapa de procesos vigente en la Universidad del Cauca [67], la institución se rige por cuatro Macro-Procesos: Procesos estratégicos, Procesos misionales, Procesos de apoyo y Procesos de evaluación. Luego, según lo establecido en el Despliegue de procesos Institucionales [68], los macro-procesos se dividen en ocho procesos, y estos a su vez se dividen en treinta y dos subprocesos.

La Tabla III ilustra la contextualización del procedimiento *Inscripciones y Admisiones* en el marco del despliegue de procesos de la Universidad del Cauca, en donde se tiene la siguiente ruta de procesos:

- Macro-Proceso: *Apoyo y Soporte*
- Proceso: *Gestión Administrativa*
- Subproceso: *Gestión admisiones, registro y control académico*
- Procedimiento: *Inscripciones y Admisiones*

Finalmente, es importante destacar que, dada la complejidad de la Universidad del Cauca, este trabajo de grado se encuentra enfocado en el procedimiento *Inscripciones y Admisiones,* específicamente a las actividades que lo componen dentro del alcance de la División de Admisiones, Registro y Control Académico DARCA.

TABLA III. Ubicación institucional del procedimiento *Inscripciones y admisiones*.

Macro Proceso	Proceso	Sub-Proceso	Procedimiento	Actividades
Estratégicos	.....	.....	.....	.....
Misionales	.....	.....	.....	.....
Apoyo/Soporte	Gestión Administrativa	.....	.....	.....
		Gestión admisiones, registro y control académico	.....	.....
			Inscripciones y Admisiones	1. Definición del calendario de admisión
				2. Justificación del servicio de aplicación de la prueba
				3. Inscripciones
				4. Alistamiento para la aplicación de la prueba
				5. Aplicación de la prueba
				6. Evaluación de la prueba
				7. Admisión y matricula
			.....	.....
		.....	.....	.....
	Gestión de la Cultura y el Bienestar	.....	.....	.....
Evaluación	.....	.....	.....	.....

2.3. MARCO TEÓRICO

2.3.1. Conceptos Preliminares

2.3.1.1. Seguridad de la Información

La norma ISO/IEC 27000:2016, define la seguridad de la información como la preservación de la disponibilidad, la confidencialidad y la integridad de la información, teniendo en cuenta las siguientes definiciones:

- **Confidencialidad**: Información disponible exclusivamente a personas autorizadas

- **Integridad**: Mantenimiento de la exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas. Contra la integridad la información puede parecer manipulada, corrupta o incompleta.

- **Disponibilidad**: Acceso y utilización de los servicios sólo y en el momento de ser solicitado por una persona autorizada.

Para lograr esto se utilizan un "conjunto coherente de procesos, normas y herramientas para la gestión eficaz de acceso a la información, y la implementación de mecanismos y medidas de seguridad tanto físicas como lógicas, orientadas a la prevención y detección de amenazas internas y externas que puedan atentar contra la seguridad de la organización y asegurar la continuidad del negocio" [69] (p.30).

Finalmente vale la pena agregar que "la seguridad de la información, no es un activo a comprar, ni un fin en sí mismo, tampoco un estado a alcanzar haciendo una determinada inversión; debe gestionarse, debe existir una meta concreta, criterios generales de evaluación y de decisión, y debe poder medirse" [70] (p.2).

2.3.1.2. Sistema de Gestión de la Seguridad de la Información - SGSI

Sistema de Gestión de Seguridad de la Información - SGSI, en ingles ISMS (Information Security Management System). La norma ISO/IEC 27000:2016 describe un SGSI como un conjunto de "políticas, procedimientos, directrices, recursos y actividades asociados, gestionados colectivamente por una organización, con el fin de proteger sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos de negocio".

Según [71] (p.20) el SGSI es un "conjunto de políticas de administración de la información basándose en el diseño, implantación y mantenimiento de procesos para gestionar eficientemente los activos de información minimizando a la vez los riesgos de seguridad de la información".

El SGSI garantiza la Seguridad de la Información mediante una estructura de buenas prácticas Mejoras [72] (p.3), definidas por: Gestión de riesgo, Políticas, Procesos, Procedimientos, Controles, Revisiones y Mejoras, con el objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir [15] (p.3).

2.3.1.3. Glosario

El conjunto de términos empleados en este trabajo de grado se han extraído de la norma ISO/IEC 27000 [73]. A continuación, se muestran los conceptos más representativos para este documento.

- **Acción correctiva:** Acción para eliminar la causa de una no conformidad y para prevenir la recurrencia.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencia de auditoría. Proceso de evaluación objetiva para determinar en qué medida se cumplen los criterios de auditoría.
- **Alta Dirección:** Persona o grupo de personas que dirige y controla una organización al más alto nivel.
- **Alcance:** Extensión y limites donde se aplica un SGSI.
- **Competencia:** Capacidad de aplicar conocimientos y habilidades para lograr los resultados deseados.
- **Conformidad:** Cumplimiento de un requisito.
- **Contexto interno:** Ambiente interno en el que la organización busca alcanzar sus objetivos.
- **Control:** Constituye las medidas o acciones encaminadas a modificar el riesgo.
- **Eficacia:** En qué medida se realizan las actividades previstas y se alcanzan los resultados previstos.
- **Gestión de la seguridad de la información:** Sistema por el cual las actividades de seguridad de la información son dirigidas y controladas.
- **Información documentada:** Información que debe ser controlada y mantenida por una organización y el medio en el que está contenida
- **Incidente de seguridad de la información:** Única o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad de comprometer las operaciones comerciales y amenazar la seguridad de la información.

- **Medida:** Variable a la que se asigna un valor como resultado de la medición
- **Medición:** Proceso para determinar un valor
- **Mejora Continua:** Actividad recurrente para mejorar el rendimiento.
- **No conformidad:** Incumplimiento de un requisito
- **Objeto de medición:** Elemento caracterizado mediante la medición de sus atributos
- **Objetivo de control:** Declaración que describe lo que se debe lograr como resultado de la implementación de controles.
- **Política:** Intenciones y dirección de una organización expresada formalmente por su alta dirección.
- **Parte interesada:** Persona u organización que puede afectar, verse afectada o percibirse afectada por una decisión o actividad.
- **Resultados de la medición:** Uno o más indicadores y sus interpretaciones asociadas que respondan a una necesidad de información.
- **Proceso:** Conjunto de actividades interrelacionadas o interactuantes que transforman los insumos en productos
- **Requisito:** Necesidad o expectativa que se indica, generalmente implícita o obligatoria
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos
- **Sistema de gestión:** Conjunto de elementos interrelacionados o interactuantes de una organización para establecer políticas y objetivos, y procesos para lograr esos objetivos
- **Declaración de Aplicabilidad – SOA (**Statement of Applicability**):** Es un documento que contiene los objetivos de control y los controles relevantes y aplicables al alcance del SGSI. El SOA se construye con base en los resultados de los procesos de evaluación y tratamiento de riesgos.
- **Tratamiento de riesgo:** Proceso para modificar el riesgo

2.3.2. Revisión Bibliográfica de la norma ISO/IEC 27001 y modelo EFQM

Esta parte sirvió para comprender la norma y el modelo en función de su aplicación en diferentes contextos organizacionales. Esta parte permite obtener un dominio de las dos temáticas, siendo fundamental para realizar una armonización entre ellas.

- **Bases de datos y términos de búsqueda**

Este proyecto de investigación tiene inmersas dos temáticas principales: La norma ISO/IEC 27001 y el modelo EFQM. Para realizar la revisión bibliográfica se ejecutó una búsqueda sobre cuatro bases de datos (Elsevier, Springer, ScienceDirect e IEEEXplorer). En la búsqueda se usaron las palabras claves como: implementar SGSI, implantar SGSI, ISO/IEC 27001, 27001:2013, norma ISO/IEC 27001:2013, Sistema de Gestión de Seguridad de la Información, Modelo EFQM, modelo europeo de excelencia, modelo de calidad total.

La búsqueda se limitó a tesis, resúmenes, palabras clave y títulos de los artículos. Para realizar toda la búsqueda y análisis de esta información se siguió la metodología expuesta en [16].

- **Criterios de selección**

Se establecieron los siguientes criterios de inclusión: publicaciones de trabajos actuales (2013 en adelante), en inglés o en español, publicados en revistas científicas. Se excluyeron aquellos artículos que se basaron en la versión 2005 de la norma ISO/IEC 27001. También se excluyeron aquellos artículos que se basaron en la versión 2003 del modelo, ya que el modelo EFQM fue reformado y modificado.

Se obtuvieron inicialmente 70 estudios como resultado de las búsquedas de las palabras clave en las bases de datos y páginas con contenido relacionado. Lugo, se excluyeron aquellos estudios no revelaron aportes significativos para los objetivos de este trabajo de grado. Finalmente se obtuvieron 50 unidades documentales entre artículos y tesis como *base de conocimiento*, lo cual permitió la investigación y análisis de la norma ISO/IEC 27001:2013 y del modelo EFQM;2013.

- **Síntesis de los datos**

El modelo EFQM no es comúnmente empleado en conjunto con las normas de la serie 27000, por lo que las unidades documentales se analizaron tomando por separado la norma ISO/IEC 27001 y el modelo EFQM.

El modelo EFQM es el modelo de calidad de origen europeo, y se emplea mayormente a nivel organizacional, es decir que se aplica para mejorar la calidad de los productos y servicios que una empresa ofrece al mercado. Además, el EFQM es un modelo no normativo, de aplicación voluntaria, que se basa en la ***autoevaluación*** de nueve criterios que el modelo establece como determinantes para instaurar la calidad.

El modelo EFQM es ampliamente utilizado y reconocido por las organizaciones de Europa. Actualmente las organizaciones que empleen dicho modelo pueden obtener un reconocimiento dado a través de unos *sellos de excelencia*[9]. Obtener un sello de excelencia representa, para una organización europea, la evidencia de una ***gestión excelente*** que se logra gracias al uso del modelo EFQM.

Por otra parte, las organizaciones de todo tipo y tamaño dependen directa o indirectamente de la información que se maneja en su interior, por lo tanto, la norma ISO/IEC 27001 ha ido ganando importancia progresivamente tanto en organizaciones de carácter público como privado. La norma ha tenido un gran auge en los últimos tiempos debido al valioso papel que desempeña un SGSI en el gobierno corporativo de las empresas. El cumplimiento de la norma permite obtener una certificación del SGSI, lo cual representa un aval en seguridad de la información para la organización certificada, generando ***prestigio***, a la vez que se mejoran las prácticas de seguridad.

2.3.3. Norma ISO/IEC 27001:2013

ISO/IEC 27001:2013 es una norma reconocida internacionalmente, emitida por la Organización de Estandarización Internacional – ISO y la Comisión Electrotécnica Internacional – IEC. La norma ISO/IEC 27001 se titula “Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos” [7].

La norma ISO/IEC 27001 establece los requisitos que debe cumplir una organización para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información - SGSI. El cumplimiento de los requisitos de la norma ISO/IEC 27001 es lo único que permite

[9] Sellos de excelencia: Comúnmente conocidos como sellos EFQM. Cada sello es un reconocimiento a las organizaciones que llevan a cabo principios de la administración de la calidad total en su actividad diaria y en las relaciones con sus stakeholders u otros grupos.

obtener la certificación de un SGSI. La última actualización de la norma ISO/IEC 27001 se realizó en el año 2013, siendo esta la versión utilizada en este trabajo de grado. La norma ISO/IEC 27001:2013 se compone de 10 cláusulas y un anexo que recomienda 114 controles agrupados en 14 dominios y 35 objetivos de control.

- **Cláusulas de la norma ISO/IEC 27001**

La norma ISO/IEC 27001 contiene 10 cláusulas que establecen los requisitos de un SGSI, siendo las cláusulas 4 a la 10 de obligatorio cumplimiento. Estas cláusulas son:

0. Introducción
1. Objetivo y campo de aplicación
2. Objetivo y campo de aplicación
3. Términos y Definiciones
4. Contexto de la organización.
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del Rendimiento
10. Mejora

- **Anexo A de la norma ISO/IEC 27001**

El Anexo A de la norma ISO/IEC 27001 se titula “objetivos de control y controles de referencia”. Este anexo contiene 114 controles que provienen del estándar ISO/IEC 27002: 2013 [9]. Los controles comunes se agrupan para dar cumplimiento a 35 objetivos de control. Teniendo en cuenta una orientación más general, los controles se agrupan en 14 dominios. Los dominios del Anexo A de la norma ISO/IEC 27001:2013 son:

A.5. Políticas de seguridad de la Información

A.6. Organización de la seguridad de la información

A.7. Seguridad de los recursos Humanos

A.8. Gestión de activos

A.9. Control de acceso

A.10. Criptografía

A.11. Seguridad física y del entorno

A.12. Seguridad de las operaciones

A.13. Gestión de las Comunicaciones

A.14. Adquisición, desarrollo y mantenimiento de sistemas

A.15. Relaciones con los proveedores

A.16. Gestión de incidentes de seguridad de la información

A.17. Aspectos de seguridad de la información de la gestión de continuidad del negocio

A.18. Cumplimiento

2.3.4. Ciclo Deming o ciclo PHVA

El ciclo Deming es conocido por las siglas PHVA (P-Planificar, H-Hacer o Ejecutar, V-Verificar, A-Actuar), en inglés PDCA (P-Plan, D-Do, C-Check, A-Act). El ciclo Deming describe un ciclo de mejora continua que se lleva a cabo a través de cuatro fases, efectuadas en orden secuencial comenzando por la fase *Planear* como lo ilustra la Fig. 4. Estas cuatro fases se encuentran estrechamente relacionadas unas con otras. La Tabla IV presenta una descripción de las fases del Ciclo Deming, comparando el enfocado hacia el SGSI y el enfoque general.

Fig. 4. Ciclo Deming de mejora continua (PHVA)

Finalmente, es importante destacar que este proyecto se encuentra enfocado únicamente en la fase *Ejecución* del SGSI. No obstante, es necesario comprender y revisar todo el ciclo, ya que las fases están estrechamente relacionadas.

TABLA IV. Descripción de las fases del ciclo PHVA enfocado en la implementación de un SGSI

Fase	Descripción PHVA	PHVA con enfoque hacia el SGSI
Planificar (establecer el SGSI)	Establecer los objetivos y procesos necesarios para obtener los resultados, de conformidad con los requisitos del cliente y las políticas de la organización [74]	Obtener soporte de la dirección de la entidad, Identificar legislación y normatividad aplicable, Definir el alcance del SGSI, Definir la política de la seguridad de la información, Análisis del riesgo, Definir la aproximación para la gestión del riesgo, Identificación de activos, Identificar los riesgos, Analizar el riesgo, Enumerar las opciones para el tratamiento/reducción del riesgo, Plan de tratamiento del riesgo y Generar la declaración de aplicabilidad [75].
Ejecutar (implementar y operar el SGSI)	Implementar procesos para alcanzar los objetivos [74].	Implementar el plan de tratamiento del riesgo, Documentar los controles del SGSI, Implementar políticas y controles de seguridad de la fase de planeación, Implementar los planes de concientización y entrenamiento, Establecer y gestionar la operación del SGSI y sus recursos [75].
Verificar (hacer seguimiento y revisar el SGSI)	Realizar seguimiento y medir los procesos y los productos en relación con las políticas, los objetivos y los requisitos, reportando los resultados alcanzados [74].	Revisiones regulares de eficacia, Revisar el nivel del riesgo residual, Realizar auditorías internas, Revisión de la dirección del SGSI y Registro del impacto en el SGSI [75].
Actuar (mantener y mejorar el SGSI)	Realizar acciones para promover la mejora del desempeño del (los) proceso(s) [74].	Implementar las mejoras identificadas y aprobadas al SGSI en un nuevo ciclo, Tomar medidas preventivas y correctivas, Aplicar las lecciones aprendidas, Comunicar los resultados, Realizar un proceso continuo y Gestión auto sostenible del modelo [75].

2.3.5. Fase *Plan* del SGSI (Realizada en el procedimiento *Inscripciones y Admisiones*)

En esta sección se presenta la recopilación de los documentos obligatorios de la fase *Plan* del SGSI realizada en el procedimiento *Inscripciones y Admisiones*, perteneciente a DARCA de la Universidad del Cauca.

Es imprescindible manifestar que la recopilación de los documentos obligatorios de la fase *Plan* del SGSI se realizó con base en el trabajo de grado titulado "*Gestión del Riesgo en la Seguridad de la Información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S. Caso de Estudio: Procedimiento de Inscripciones y Admisiones en la División de Admisión Registro y Control Académico (DARCA) de la Universidad del Cauca*" [76]. Se aclara también que algunos de los documentos obligatorios fueron complementados y/o modificados en el desarrollo del presente trabajo de grado, para obtener así, los registros especificados en la norma ISO/IEC 27001, en su versión de 2013. A continuación, se describe cada uno de los documentos obligatorios de la fase *Plan* del SGSI.

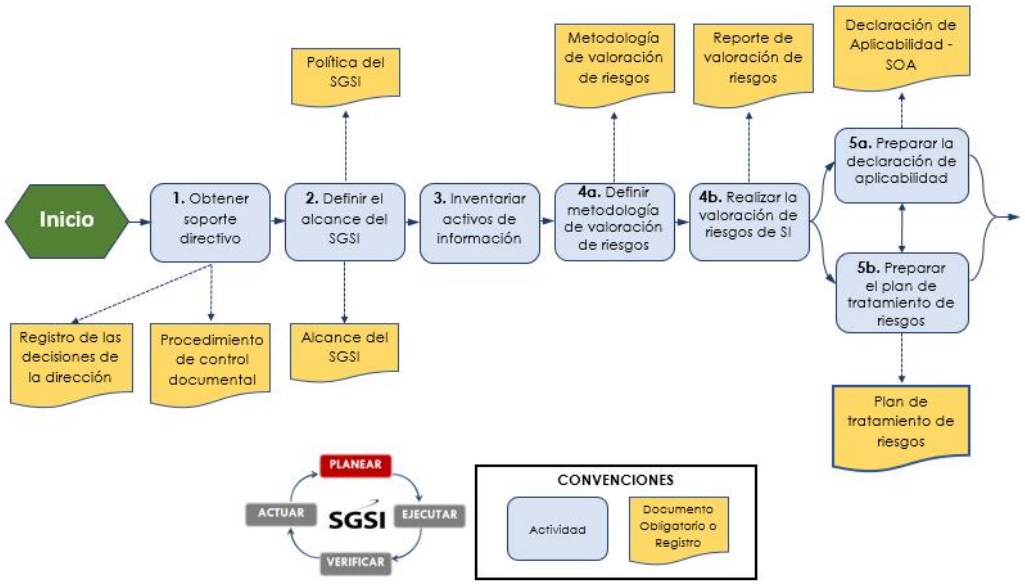

Fig. 5. Actividades y documentos obligatorios de la Fase *Plan* de un SGSI. [77]

Para comprender la fase *Plan* del SGSI llevada a cabo en el procedimiento *Inscripciones y Admisiones* de DARCA de la Universidad del Cauca se emplea la Fig. 5, en donde se ilustra un conjunto de actividades específicas y los ***documentos***

obligatorios[10] asociados a las actividades, con base en los requisitos de la norma ISO/IEC 27001: 2013. Las actividades que le corresponden a la fase *Plan* del SGSI son las siguientes:

1. Obtener soporte Directivo
2. Definir el Alcance del SGSI
3. Inventariar activos de información
4.a. Definir metodología de valoración de riesgos
4.b. Realizar valoración de riesgos de seguridad de la información
5.a. Preparar la declaración de aplicabilidad
5.b. Preparar el plan de tratamiento de riesgos

Los *documentos obligatorios* que se muestran en la Fig. 5 constituyen los resultados medibles que evidencian el cumplimiento de la fase *Plan* del SGSI. Estos documentos obligatorios son:

- Registros de las decisiones de la dirección
- Procedimiento de control documental
- Alcance del SGSI
- Política del SGSI
- Metodología de valoración de riesgos
- Reporte de valoración de riesgos
- Declaración de aplicabilidad - SOA
- Plan de tratamiento de riesgos

2.3.5.1. Registros de las decisiones de la dirección

Como ilustra la **Fig. 5**, la actividad número uno para el desarrollo de la fase *Plan* del SGSI es "Obtener soporte Directivo", y como documento obligatorio asociado se encuentran los *Registros de las decisiones de la Dirección.*

En los registros de la fase *Plan* del SGSI no se encontraron evidencias de las decisiones de la dirección, y esto representa un vacío según los documentos obligatorios especificados en la Fig. 5. Por lo tanto, se realizó un "Acta de inicio del proyecto del SGSI" para el procedimiento *Inscripciones y Admisiones* de DARCA de

[10] Documento Obligatorio: Constituye un registro que evidencia el cumplimiento de una actividad, y por medio del cual se da cumplimiento a una cláusula de la norma ISO/IEC 27001.

la Universidad del Cauca, la cual se puede ver en la primera sección del ***Anexo A***. Esta acta describe los actores que intervienen en el proyecto y se definen las responsabilidades del jefe de DARCA quien encabeza y dirige el SGSI. Esta esta acta fue realizada el 17 de abril de 2017.

2.3.5.2. Procedimientos de control documental

Como muestra la **Fig. 5**, la actividad número uno para el desarrollo de la fase *Plan* del SGSI es "Obtener soporte Directivo", y como documento obligatorio asociado se encuentra *Procedimientos de Control Documental*.

La Universidad del Cauca cuenta con un *Procedimiento de Control Documental*, el cual aplica para DARCA. Este procedimiento se titula "Elaboración y Control de Documentos" [78], identificado con el código PE-GS-2.2.1-PR-1 y su propósito es establecer una guía para administrar los documentos internos de la Universidad especificando la estructura, diseño, codificación, elaboración, revisión y aprobación de los documentos, además de las modificaciones realizadas.

2.3.5.3. Alcance del SGSI

Como muestra la **Fig. 5**, la actividad número dos para el desarrollo de la fase *Plan* del SGSI es "Definir el alcance del SGSI", y como documento obligatorio asociado se encuentra el *Alcance del SGSI.*

EI alcance para el procedimiento *Inscripciones y Admisiones* de DARCA de la Universidad del Cauca [41] (pp.36-37) se muestra en la Fig. 6. En este orden de ideas, el procedimiento *Inscripciones y Admisiones* se compone de actividades que se interrelacionan entre sí. Cada acción realizada en una actividad depende de la actividad anterior e influye sobre la actividad posterior. Así pues, las actividades del procedimiento en mención son las siguientes, según [14] (pp.27-40):

1. Definición del calendario de admisión
2. Justificación del servicio de aplicación de la prueba
3. Inscripciones
4. Alistamiento para la aplicación de la prueba
5. Aplicación de la prueba
6. Evaluación de la prueba
7. Admisión y Matricula

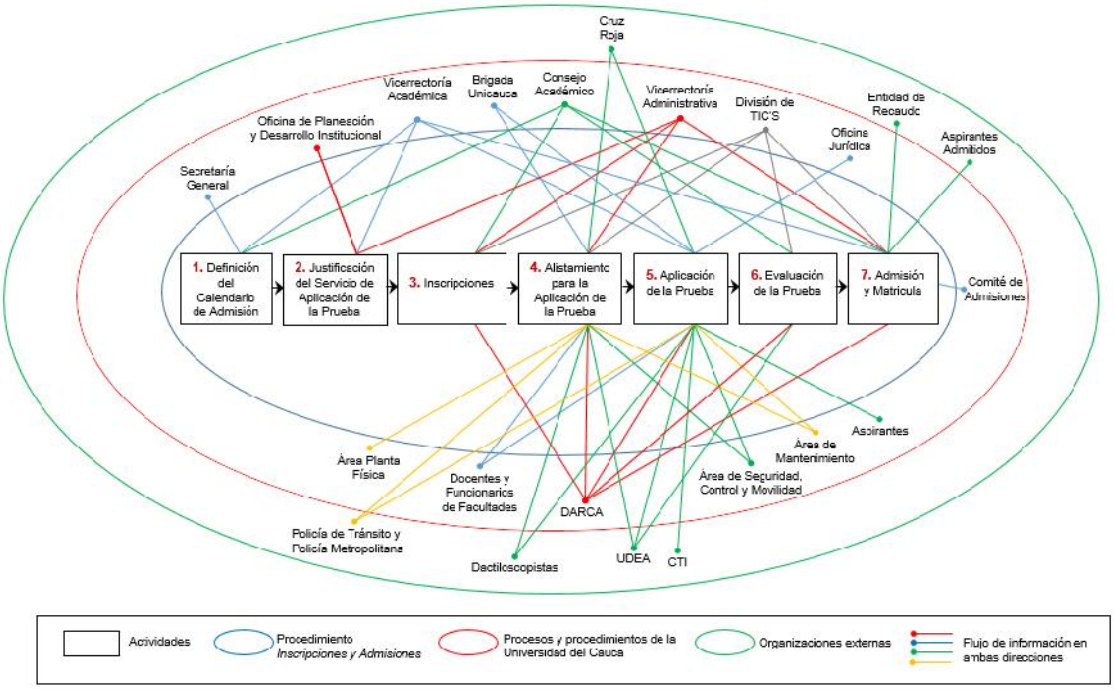

Fig. 6. Alcance del procedimiento *Inscripciones y Admisiones*. [79] (p.37)
Fuente Modificada

El alcance del SGSI para procedimiento *Inscripciones y* Admisiones se ilustra empleando el método de las elipses, permitiendo identificar interacciones de las actividades con entidades internas y externas a la Universidad del Cauca.

Cabe resaltar que el alcance del SGSI mostrado en la Fig. 6 sirve para comprender la complejidad del procedimiento *Inscripciones y Admisiones.* Es preciso resaltar que todas las actividades del procedimiento en mención son de singular importancia DARCA, sin embargo, los resultados de la valoración de riesgos en la fase *Plan* del SGSI para el procedimiento *Inscripciones y Admisiones* de DARCA [14] arrojaron que las actividades con mayor nivel de riesgo son en su respectivo orden:

1. Evaluación de la Prueba. (Mayor nivel de riesgo)
2. Inscripciones
3. Aplicación de la Prueba
4. Alistamiento para la aplicación de la prueba
5. Admisiones

2.3.5.4. Política del SGSI

Como muestra la **Fig. 5**, la actividad número dos para el desarrollo de la fase *Plan* del SGSI es “Definir el alcance del SGSI”, y como documento obligatorio asociado

se encuentra la *Política del SGSI.* Cabe mencionar que la implementación exitosa del SGSI depende en gran manera de la política. Esta sección se divide en dos partes, la primera presenta la política de alto nivel para toda la Universidad del Cauca, y que por ende es de aplicabilidad para DARCA. La segunda parte presenta la política elaborada específicamente para el procedimiento *Inscripciones y Admisiones* de DARCA.

- ✓ **Política del Sistema de Gestión de la Seguridad de la Información de la Universidad del Cauca**

La política titulada "Sistema de Gestión de la Seguridad de la Información de la Universidad del Cauca" fue establecida bajo resolución R-785 del 7 de Octubre de 2015 [80]. Vale la pena aclarar que ésta política es el resultado del esfuerzo realizado por el Ingeniero *Siler Amador Donado* en conjunto con el Ingeniero *Francisco Javier Terán*. También es preciso aclarar que esta política se realizó por fuera de la fase *Plan* del SGSI del procedimiento *Inscripciones y Admisiones* de DARCA.

La política del SGSI de la Universidad del Cauca es un documento de alto nivel que involucra a toda la institución, sus estamentos universitarios, contratistas, proveedores y ciudadanía en general. Por lo tanto, es de aplicabilidad en el procedimiento *Inscripciones y Admisiones,* perteneciente a DARCA de la Universidad del Cauca. Esta política cumple con la regulación colombiana para la seguridad de la información, es corta, concisa, fácil de comprender y establece las directrices que se deben cumplir para la implementación de un SGSI dentro de la universidad.

- ✓ **Política de Seguridad de la Información del procedimiento *Inscripciones y Admisiones* de DARCA**

La *Política de seguridad de la Información* establecida en la fase *Plan* del SGSI para el procedimiento *Inscripciones y Admisiones* de DARCA [79] (pp.27-34) es un documento cuyo objetivo es "guiar la implementación de medidas que protejan los activos informáticos, manteniendo la integridad, confidencialidad y disponibilidad de los datos dentro de los sistemas de aplicación, redes e instalaciones de cómputo".

La *Política de seguridad de la Información* definida para el procedimiento *Inscripciones y Admisiones* contiene un conjunto de políticas enfocadas en el ámbito de las responsabilidades operacionales, el control de acceso a datos y la información almacenada en medios digitales.

2.3.5.5. Metodología de valoración de riesgos

Como muestra la **Fig. 5**, la actividad número 4a para el desarrollo de la fase *Plan* del SGSI es “Definir la metodología de Valoración de Riesgos”, y como documento obligatorio asociado se encuentra la *Metodología de Valoración de Riesgos.*

La metodología empleada para realizar la Valoración de riesgos en el procedimiento *Inscripciones y Admisiones* fue OCTAVE-S (**O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation - **S**mall) [81], la cual aprovecha los conocimientos de las personas a favor de la seguridad de la información. La metodología OCTAVE-S empleada por los investigadores *Martinez Pulido* y *Espinosa Tafur* [14] es de vital importancia en todo el ciclo que describe el Modelo PHVA para el SGSI, ya que define las acciones a realizar durante todo el proceso de implementación de un SGSI.

Finalmente se destaca, que gracias al proceso de la valoración de riesgos realizado con la metodología OCTAVE-S se definieron los planes para la mitigación de riesgos, siendo estos los insumos fundamentales que describen las acciones a realizar en la fase *Ejecución* del SGSI.

2.3.5.6. Reportes de valoración de riesgos

Como muestra la **Fig. 5**, la actividad 4b para el desarrollo de la fase *Plan* del SGSI es “Definir la metodología de Valoración de Riesgos”, y como documento obligatorio asociado se encuentra el *Reporte de Valoración de Riesgos.*

Este documento obligatorio fue realizado en el transcurso del presente trabajo de grado. En este sentido, el *Reporte General de Valoración de Riesgos* elaborado se muestra en la segunda sección del ***Anexo A***. Este reporte toma como base el artículo final [82] del proyecto fase *Plan* del SGSI para el procedimiento *inscripciones y Admisiones*.

Por una parte, el *Reporte General de Valoración de Riesgos* muestra la correspondencia entre las directrices de la norma ISO/IEC 27005 de 2011 con las fases y actividades de la metodología OCTAVE-S. Por otra parte, el reporte define un conjunto de actividades para construir los perfiles de amenaza, identificar las vulnerabilidades de la infraestructura y finalmente desarrollar planes de mitigación de riesgos. Como resultado de todo el proceso de valoración del riesgo también se construye la Declaración de Aplicabilidad.

2.3.5.7. Declaración de Aplicabilidad - SOA[11]

Como muestra la **Fig. 5**, la actividad número 5a para el desarrollo de la fase *Plan* del SGSI es "Preparar la declaración de aplicabilidad", y como documento obligatorio asociado se encuentra la propia *Declaración de Aplicabilidad.*

Este documento obligatorio fue realizado en el transcurso del presente trabajo de grado. En este sentido, la *Declaración de Aplicabilidad* elaborada se muestra en la tercera sección del ***Anexo A***. Esta decisión obedeció a que el SOA realizado en la fase Plan del SGSI [79] (pp.17-26) lista absolutamente ***todos*** los controles especificados en el anexo A de la norma ISO/IEC 27001:2005.

Con el SOA elaborado se completan apropiadamente los documentos obligatorios expuestos en la Fig. 5. El SOA realizado incluye únicamente 28 controles de los 114 encontrados en el Anexo A de la norma ISO/IEC 27001:2013. El objetivo de la declaración de aplicabilidad es precisamente enfocarse en los controles más relevantes para el procedimiento *Inscripciones y Admisiones*, prestando especial atención a aquellos que más se necesitan.

2.3.5.8. Plan de tratamiento de riesgos

Como muestra la **Fig. 5**, la actividad número 5b para el desarrollo de la fase *Plan* del SGSI es "Preparar el Plan de Tratamiento de Riesgos", y como documento obligatorio asociado se encuentra el *Plan de Tratamiento de Riesgos.*

Entre las opciones de tratamiento de riesgos (Aceptar, Mitigar, Eliminar) que se tuvieron en cuenta en la fase *Plan del SGSI* para el procedimiento *Inscripciones y Admisiones* [1] (p.102) se seleccionó la opción "Mitigar". Por lo tanto en [1] (pp.112-128) se muestran los *Planes de mitigación de Riesgos.*

El *Plan de tratamiento de* Riesgos da cumplimiento al requisito número 6.1.3.e)[12] de la norma ISO/IEC 27001:2013 y señala acciones y actividades que han sido diseñadas para reducir los riesgos que podrían impedir que el procedimiento *Inscripciones y Admisiones* en DARCA logre su misión.

---

[11] Declaración de Aplicabilidad – SOA: Es un documento que lista los objetivos de control y controles de seguridad recomendados para lograr la reducción del riesgo a nivel aceptable

[12] Clausula 6.1.3.e) de la norma ISO/IEC 27001:2013. Formular un plan de tratamiento de riesgos de la seguridad de la información.

2.3.6. Fase *Ejecución* de un SGSI

La fase *Ejecución* de un SGSI corresponde a la segunda fase del ciclo Deming. Para comprender la fase *Ejecución* del SGSI a ser desarrollada en el procedimiento *Inscripciones y Admisiones* de DARCA de la Universidad del Cauca se emplea la Fig. 7, la cual ilustra un conjunto de actividades específicas, y los documentos obligatorios asociados a esas actividades, con base en los requisitos de la norma ISO/IEC 27001: 2013.

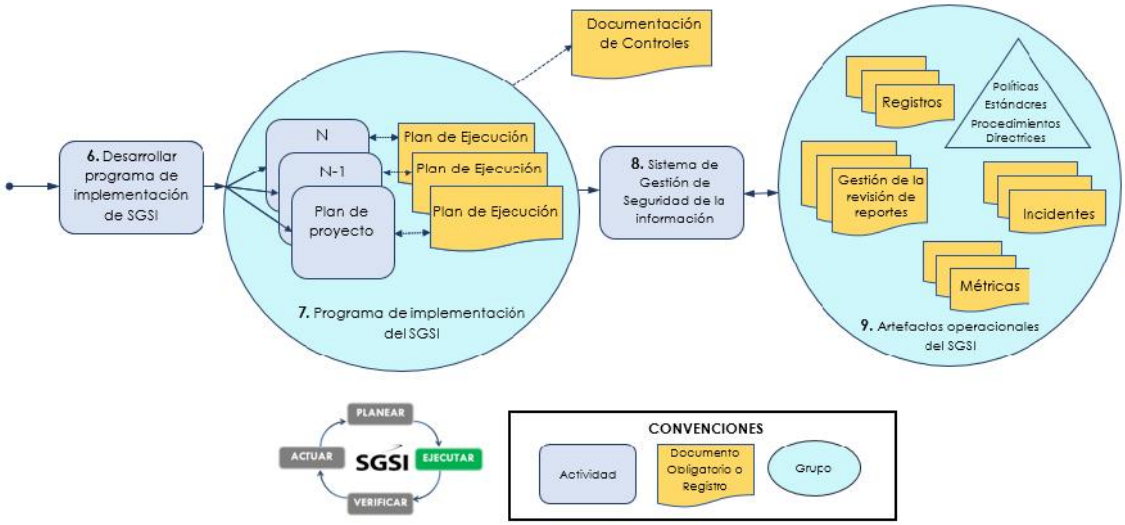

Fig. 7. Actividades y documentos obligatorios de la fase *Ejecución* de un SGSI. [77]

Siguiendo con la numeración establecida en la Fig. 5, las actividades que le corresponden a la fase *Ejecución* del SGSI son las siguientes:

6. Desarrollar el programa de implementación del SGSI
7. Ejecutar el Programa de implementación del SGSI.
8. Operar el SGSI
9. Elaborar y emplear los Artefactos operacionales del SGSI

Los *documentos obligatorios* que se muestran en la Fig. 7 constituyen los resultados medibles que evidencian el cumplimiento de la fase *Ejecución* del SGSI. Es imprescindible manifestar que los documentos obligatorios en mención se deben obtener para el procedimiento *Inscripciones y Admisiones* de DARCA, siguiendo con la línea trazada en la fase *Plan* del SGSI. Estos documentos obligatorios son:

- Planes de Ejecución
- Documentación de Controles
- Artefactos operacionales

A continuación, se describe cada uno de los documentos obligatorios de la fase *Ejecutar* del SGSI.

2.3.6.1. Planes de Ejecución

Como ilustra la **Fig. 7**, la actividad número seis de la fase *Ejecución* del SGSI es "Desarrollar programa de implementación del SGSI". Esta actividad se compone de un conjunto de actividades denominadas "Planes de proyecto". En este sentido, por cada plan de proyecto (es decir por cada control seleccionado del SOA) es necesario establecer un documento obligatorio denominado *Plan de Ejecución.* Luego, es preciso elaborar un *Plan de Ejecución* por cada control a implementar, en donde se establezca un cronograma, personal, tiempo y recursos.

El conjunto de actividades que conllevan a elaborar los *Planes de Ejecución* es lo que comúnmente se conoce como "Programa de implementación del SGSI". Finalmente, es preciso aclarar que los *Planes de Ejecución* se encuentran directamente relacionados con los planes de tratamiento de riesgos provenientes de la fase *Plan* del SGSI.

2.3.6.2. Documentación de controles

Como ilustra la **Fig. 7**, la actividad número siete de la fase *Ejecución* del SGSI es el "Programa de implementación del SGSI", y como documento obligatorio asociado se encuentra la *Documentación de controles*.

La *Documentación de controles* se obtiene gracias al desarrollo de los *Planes de Ejecución*. En otras palabras, la documentación de los controles constituye los registros que corroboran la puesta en marcha de los *Planes de Ejecución*. Es preciso resaltar que la fase *Ejecución* de un SGSI se centra especialmente en la implementación de controles, para lo cual se llevan a cabo actividades que deben ser debidamente documentadas y registradas en aras de corroborar y medir la eficacia de los controles.

2.3.6.3. Artefactos operacionales

Como muestra la **Fig. 7**, la actividad número ocho de la fase *Ejecución* del SGSI es "Operar el SGSI". La actividad ocho se encuentra directamente relacionada con la actividad nueve que corresponde a "Artefactos operacionales del SGSI", y los documentos obligatorios asociados son:

- Registros
- Métricas
- Incidentes
- Procedimientos

✓ **Registros**

Los registros constituyen todos los documentos relacionados con la seguridad de la información que merecen ser almacenados por su importancia, como por ejemplo registros de asistencia a capacitaciones, registros de incidentes, actas, informes, peticiones, quejas, recomendaciones, y demás.

✓ **Métricas**

La fase Ejecución de un SGSI se centra en la implementación de controles. Las métricas constituyen una técnica que se emplea para determinar la eficacia de los controles implementados, y de manera general, la eficacia del SGSI.

La norma ISO/IEC no dice cómo hacer la medición, por lo tanto, se debe seleccionar una metodología, norma, estándar, guía o práctica (es decir un marco de referencia) para dar cumplimiento a esta parte. Es en esta parte donde el modelo EFQM entra a apoyar la norma por medio de la autoevaluación constante.

✓ **Incidentes**

Este documento constituye los reportes de los aspectos más relevantes de un incidente ocurrido que afecta la organización. Un incidente de seguridad de la información puede ser un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información.

✓ **Procedimientos**

Los *Artefactos operacionales* del SGSI corresponden a un conjunto de documentos obligatorios denominados “Procedimientos” que definen el paso a paso a seguir. Entre los procedimientos se tiene:

- Procedimiento de Control de Registros
- Procedimiento operativo del SGSI
- Procedimiento de auditoria interna del SGSI.
- Procedimiento de acción preventiva

- Procedimiento de acción correctiva
- Procedimiento de las comunicaciones
- Gestión de la revisión de reportes.

- **Procedimiento de control de registros**

El *procedimiento de control de registros* está relacionado con el manejo de todo tipo de documentos que corresponden al SGSI. Este procedimiento establece los pasos que se deben seguir para ordenar y controlar la documentación generada en el SGSI. El procedimiento de control de registros es un documento que brinda las especificaciones para el almacenamiento, la protección, la recuperación, el tiempo de retención y la disposición de los registros del SGSI.

- **Procedimiento operativo del SGSI**

El procedimiento operativo del SGSI es un documento que establece las acciones que se deben realizar para asegurar la operación adecuada del SGSI dentro del alcance establecido. En nuestro caso, define el cómo se debe operar el SGSI dentro del procedimiento *Inscripciones y Admisiones.* Este procedimiento tiene como propósito establecer una estructura para llevar a cabo las prácticas y los procedimientos del SGSI de conformidad con la norma ISO/IEC 27001. Este procedimiento es conocido como “Manual se seguridad de la información”

- **Procedimiento de auditoria interna del SGSI.**

El procedimiento de auditoria interna del SGSI es un documento cuyo propósito es describir todas las actividades que se deben llevar a cabo para desarrollar las auditorias del SGSI al interior de la organización, en este caso al interior del procedimiento *Inscripciones y Admisiones*.

- **Procedimiento de acción preventiva**

El documento obligatorio *procedimiento de acción preventiva* está estrechamente relacionado con el *procedimiento de auditoría interna del SGSI*. Al desarrollar la auditoría interna del SGSI es posible identificar unas *no conformidades*[13] ***potenciales***. Por lo tanto, el procedimiento de acción preventiva describe una serie

[13] No conformidad (NC): Es un incumplimiento de un requisito del SGSI según la norma ISO/IEC 27001. El incumplimiento se basa en la usencia o fallo en implantar y mantener uno o más requisitos del SGSI.

de pasos que se deben llevar a cabo para darle tratamiento a la no conformidad identificada. El procedimiento se enfoca en identificar las acciones necesarias para eliminar la situación que causó la no conformidad.

- **Procedimiento de acción correctiva**

El documento obligatorio *procedimiento de acción correctiva* está estrechamente relacionado con el desarrollo de una auditoría externa del SGSI. Al desarrollar una auditoria externa es posible identificar no conformidades ***reales***. El procedimiento de acción correctiva describe una serie de pasos que se deben llevar a cabo para darle tratamiento a la no conformidad identificada. El procedimiento se enfoca en identificar las acciones necesarias para eliminar la situación que causó la no conformidad.

- **Procedimiento de las comunicaciones internas y externas**

Este procedimiento se encarga de gestionar la forma en que se va a presentar a información de DARCA hacia las partes interesadas que pueden encontrarse al interior o exterior de la dependencia, que pueden ser aspirantes, estudiantes, docentes, funcionarios, y demás. Las comunicaciones internas se realizan desde la división de DARCA hacia otras divisiones o comunidad universitaria. La comunicación externa trata documentos emitidos por alguna sección de DARCA para informar a un ente externo de un tema que se considera importante en relación a la seguridad de la información

- **Gestión de la revisión de reportes.**

Este documento es un informe que representa las principales conclusiones y recomendaciones después de que la dirección, o la persona competente realiza la revisión y análisis de los reportes de seguridad de la información.

2.3.6.4. Consideraciones de la fase Ejecución del SGSI

- La norma ISO/IEC 27001 no dice cómo hacer los "***procedimientos***" descritos anteriormente, por lo tanto, para dar cumplimiento a estos documentos obligatorios se emplearon las guías proporcionadas por el *Modelo de Seguridad y Privacidad de la Información – MSPI* [83], desarrollado por el Ministerio de TIC de Colombia.

- La norma ISO/IEC 27001 no dice cómo hacer las "***Métricas de SI***", por lo tanto, para dar cumplimiento a este documento obligatorio se empleó el enfoque de autoevaluación proporcionado por el modelo EFQM.

- Adicionalmente a lo ilustrado en la Fig. 5 y la Fig. 7, la norma ISO/IEC 27001:2013 establece los requisitos "***Competencia***[14]" y "***Toma de conciencia***[15]", por lo tanto, para dar cumplimiento a estos dos requisitos fue necesario realizar capacitaciones y para ello siguieron algunas recomendaciones planteadas por la metodología NIST SP 800-50 [84].

2.3.7. Modelo EFQM

El modelo EFQM es la versión europea para la Gestión de la Calidad Total [85]. El nombre del modelo proviene de la fundación que lo creó: Fundación Europea para la Gestión de la Calidad, en inglés, *European Foundation for Quality Management.* El modelo EFQM. El modelo fue creado en 1991 y ha venido evolucionando a través del tiempo, actualizándose y ajustándose a las variaciones del mundo empresarial. La última revisión del Modelo EFQM se realizó en el año 2013, siendo esta versión empleada en este proyecto de investigación.

El modelo EFQM es muy amplio y está compuesto por tres elementos que se complementan y se despliegan estableciendo un ciclo de mejora continua. Estos tres elementos son: Principios fundamentales de calidad total, criterios y esquema lógico REDER.

2.3.7.1. Principios Fundamentales de Calidad Total/ Conceptos Fundamentales de la Excelencia

El modelo EFQM se basa en ocho principios de la Gestión de la Calidad Total, también conocidos como conceptos fundamentales de la excelencia. Estos principios son:

1. Añadir valor para los clientes
2. Crear un futuro sostenible
3. Desarrollar la capacidad de la organización
4. Aprovechar la creatividad y la innovación

[14] Competencia: Clausula 7.2 de la norma ISO/IEC 27001

[15] Toma de Conciencia: Clausula 7.3 de la norma ISO/IEC 27001

5. Liderar con visión, inspiración e integridad
6. Gestionar con agilidad
7. Alcanzar el éxito mediante el talento de las personas
8. Mantener en el tiempo resultados sobresalientes

2.3.7.2. Criterios

El modelo EFQM está compuesto por nueve criterios, frente a los cuales se evalúa el progreso de la organización hacia la excelencia. Los nueve criterios del Modelo EFQM se dividen en dos grupos: *Agentes facilitadores* y *Resultados,* tal como muestra la Fig. 8. Los *Agentes Facilitadores* representan las acciones, medios y actividades que la organización pone en marcha para obtener unos determinados resultados. Los *Resultados* son consecuencia de las acciones realizadas en los Agentes Facilitadores. Al realizar un análisis de los resultados obtenidos, se identifican oportunidades de mejora (Aprendizaje, Creatividad e Innovación) y se procede a planificar las acciones pertinentes que serán aplicadas sobre los criterios Agentes Facilitadores, iniciando otro ciclo.

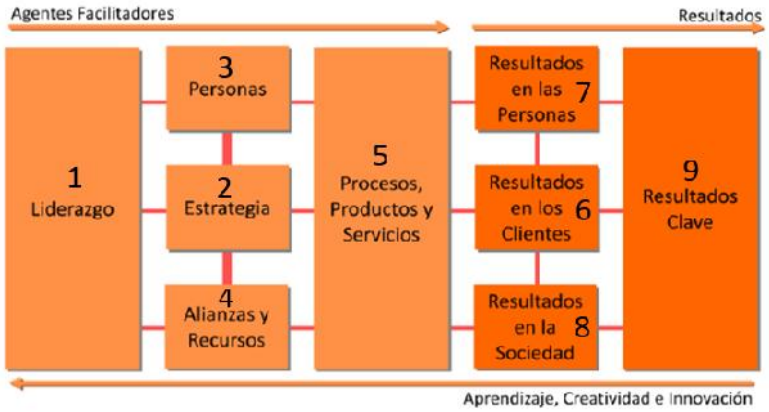

Fig. 8. Criterios del modelo EFQM. [85]

Los criterios se dividen en 32 subcriterios, que se utilizan para estructurar una visión sistemática y plena de las capacidades que plantea una organización.

2.3.7.3. Esquema lógico REDER de evaluación y puntuación.

Enfoque, Despliegue, Evaluación-Revisión, Resultados - REDER, en inglés *Results, Approach, Deployment and Assessment-Review* - RADAR. El esquema lógico REDER es una herramienta de gestión en donde se estructura la manera de evaluar el rendimiento de una organización, estableciendo un ciclo de mejora continua.

REDER sugiere como primera medida, determinar los resultados que se quieren alcanzar (los objetivos). REDER describe un proceso sistemático de mejora continua que se muestra en la Fig. 9, y se aplica sobre los criterios Resultados y Agentes Facilitadores con fines de autodiagnóstico.

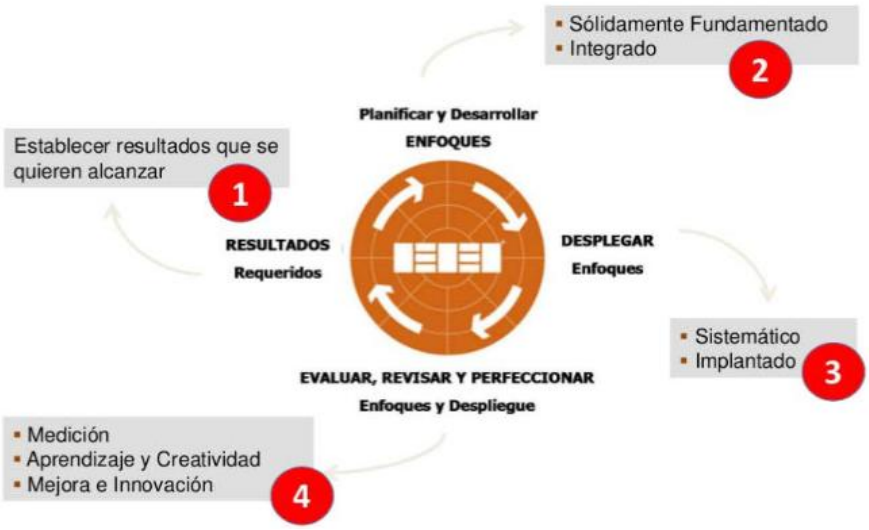

Fig. 9. Esquema lógico REDER. [86]

2.3.8. Marco de integración – HFramework

Debido a que la norma ISO/IEC 27001 y el modelo EFQM cuentan con estructuras y terminologías diferentes, se definió el uso de una marco general denominado "marco de armonización" HFramework [22], el cual permitió establecer las relaciones y diferencias para llevar a cabo una adaptación, y con ello poder reducir la subjetividad.

HFramework define los elementos necesarios para apoyar la armonización de múltiples modelos o estándares. Este marco tiene tres componentes tal como se ilustra en la Fig. 10: Marco conceptual, marco metodológico y entorno tecnológico.

- ✓ **Primero: Marco conceptual**

El marco conceptual proporciona un conjunto de términos base que permiten comprender la complejidad de la armonización de múltiples modelos. En esta parte se han establecido dos ontologías para la armonización de modelos múltiples.

- **Ontología de Armonización de Múltiples Modelos (H2mO):** Ontología que define los principales conceptos que pueden ser utilizados en un proyecto de armonización de modelo múltiples. H2mO propone una conceptualización común

de los Métodos ampliamente utilizados, técnicas, conceptos, relaciones y términos relacionados.

- **Ontología para la Gestión de Procesos (PrMO):** Ontología que establece los elementos clave utilizados para gestionar y expresar enfoques basados en procesos. El PrMO se utiliza para definir una plantilla de Estructura Común de Elementos de Proceso (CSPE[16]), la cual se aplica mediante un Método de Homogeneización (HoMethod), cuya intención es ajustar la armonización de las diferencias de los diferentes modelos.

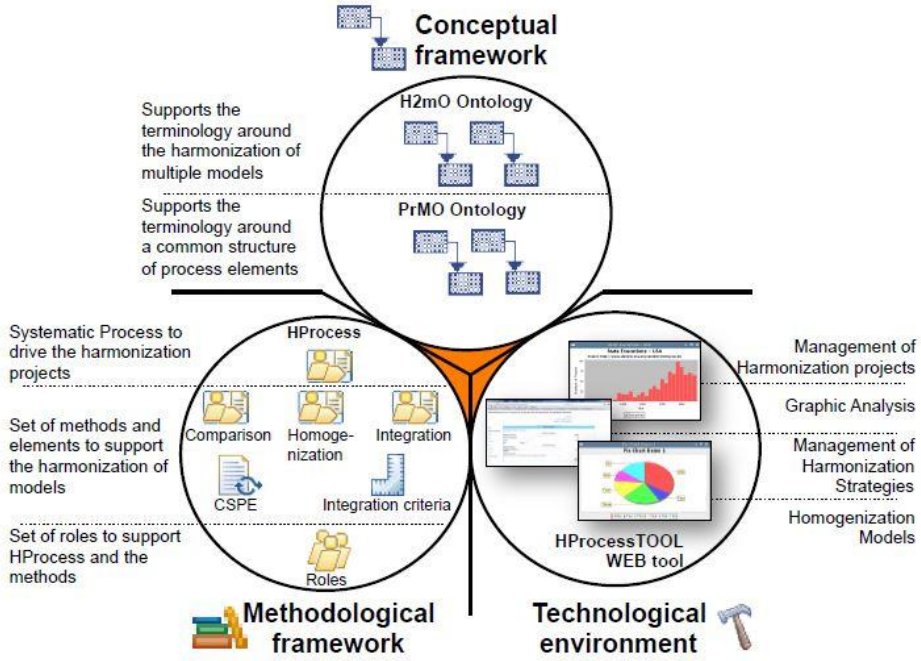

Fig. 10. Esquema de HFramework**.** [22] (p.61)

✓ Segundo: Marco metodológico

Permite la conducción y dirección sistemáticas de las actividades, tareas y funciones necesarias para apoyar los esfuerzos relacionados con la gestión y configuración de una estrategia de armonización adecuada que permita llevar a cabo la armonización de modelos múltiples. El marco metodológico contiene siguientes elementos:

[16] Estructura Común de Elementos de Proceso – CSPE: Plantilla definida para los procesos definidos en PrMO. Permite colocar múltiples modelos en la misma estructura, facilitando su mapeo e integración.

- **Proceso de armonización (HProcess):** Proceso que define paso a paso la manera de definir e implementar una estrategia de armonización - ***HStrategy*** adecuada que permitirá obtener la armonización de varios modelos o estándares. ***HProcess es la columna vertebral que establece los medios para integrar todos los elementos definidos en HFramework***, por lo tanto, en la sección 2.3.9 se describen las actividades de HProcess. Luego, ***HStrategy es el principal producto de trabajo resultante de la implementación de HProcess***, y en este sentido la armonización entre modelo EFQM y de la norma ISO/IEC 27001 se enfoca específicamente en HStrategy.

- **Métodos de armonización (HMethods)**: Conjunto de métodos, técnicas y elementos que proporcionan información sobre "cómo poner" dos o más modelos en consonancia. Los HMethods constituyen un complemento para el HProcess, por lo tanto, soportan la configuración de HStrategy. Los métodos que define HMethods son los siguientes:

  a. Homogenization Method (HoMethod*):* Método de **Homogenización**. Proporciona un conjunto de actividades que pueden ser empleadas para aplicar y poner en armonía las diferencias estructurales entre modelos a través de una *Estructura Común de Elementos de Proceso* (CSPE).

  b. Mapping Method (MaMethod): Método de **Comparación**. Permite la cartografía de los modelos.

  c. Método de Integración (IMethod): Método de **Integración**. Permite unificar las prácticas de múltiples modelos.

  ✓ **Tercero: Entorno Tecnológico**

Consiste en una Herramienta de Armonización de Procesos - **HProcessTOOL**, es decir, una herramienta WEB que permite apoyar, gestionar, controlar y supervisar un proyecto de armonización. HProcessTOOL ha sido diseñado a partir de los elementos definidos en HFramework.

2.3.9. Proceso de armonización: HProcess

Para realizar la armonización del modelo EFQM y la norma ISO/IEC 27001 se toma como base los dos primeros elementos establecidos en HFramework [22]. En primera instancia, se adopta el *marco conceptual* que define la ontología H2mO y

PrMO [60], las cuales establecen una terminología común y una plantilla autónoma cuyo propósito es favorecer la armonización de múltiples modelos.

"*HProcess es la columna vertebral que establece los medios para integrar todos los elementos definidos en HFramework",* por lo tanto, se procede a describir HProcess que constituye el marco metodológico según lo expuesto en ilustra Fig. 10. HProcess detalla el camino a seguir para alcanzar la armonización de modelos múltiples [61]. En este orden de ideas, es preciso resaltar que los dos primeros objetivos planteados en este trabajo de grado, planteados en la sección 1.2.2, se alcanzan empleando el proceso HProcess.

HProcess detalla paso a paso el proceso mediante el cual se logra la armonización de modelos múltiples, gracias al cumplimiento de actividades, responsabilidades y generación de los productos de trabajo, tal como lo ilustra la Fig. 11. Las actividades A1, A2, A3, A4 que componen HProcess se muestran con mayor detalle en la Fig. 12, permitiendo tener una mejor comprensión de su relación con los roles, productos de trabajo y otros elementos que componen el proceso de armonización empleado para el desarrollo de este trabajo de grado.

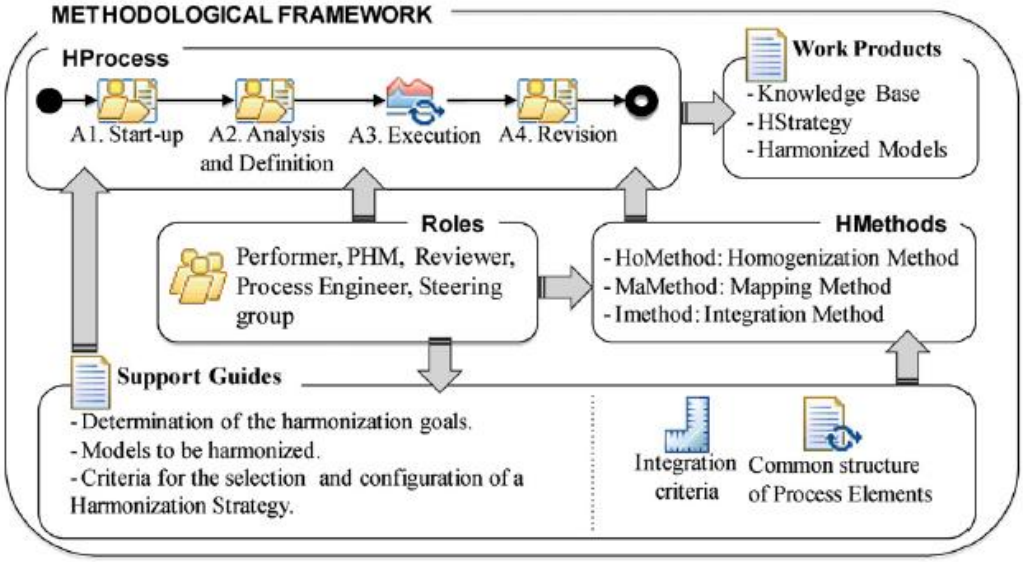

Fig. 11. HProcess para la armonización de modelos múltiples**.** [63] (p.127)

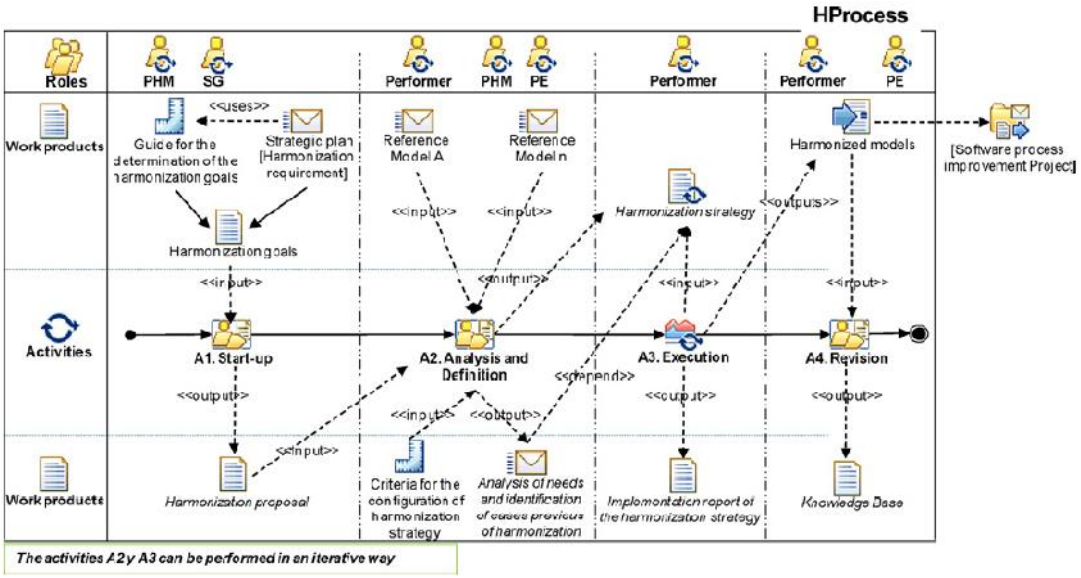

Fig. 12. Proceso para la conducción de la armonización de modelos múltiples. [63] (p.129)

2.3.9.1. Actividades de HProcess

A continuación, se presenta una descripción general de las cuatro actividades de la Fig. 12, realizada por Pardo C., según [63].

A1. Puesta en Marcha:

En esta actividad la persona responsable de la *Gestión del Proceso de Armonización* - **PHM** define una propuesta de armonización en la que se describen los elementos necesarios para guiar a la organización. La propuesta debe ser aprobada por el Grupo Directivo - **SG**.

A2. Análisis y definición:

En esta actividad el PHM y el Ejecutante - **P** realizan la priorización de los requisitos de armonización. P y el Ingeniero de Procesos - **PE** identifican los métodos de armonización a emplear. El PE busca métodos empleados anteriormente, finalmente se define una Estrategia de Armonización – **HStrategy**. En esta segunda actividad se establece la direccionalidad de la armonización.

A3. Ejecución:

P gestiona y ejecuta HStrategy, definiendo métodos y actividades para armonizar los modelos múltiples. En esta parte se redactan las lecciones aprendidas un informe de aplicación de la estrategia de armonización[17].

[17] Informe de HStrategy: información relevante sobre las actividades, objetivos, iteraciones, incidentes, soluciones y sugerencias que han ocurrido

A4. Revisión:

En esta actividad se analizan los elementos relacionados con la ejecución. P, PHM y PE obtienen una retroalimentación de las lecciones aprendidas.

2.3.9.2. Roles

A continuación, se presenta una la descripción general de los roles que se ilustran en la Fig. 12, realizada por Pardo C., según [63].

P – Performer: Ejecutante. Persona responsable del análisis de modelos, que implementa la armonización. Esta persona debe tener capacidades para la abstracción, análisis de modelos, relacionar y comparar modelos.

PE – Process Engineer: Ingeniero de Procesos. Persona responsable de llevar a cabo actividades relacionadas con la definición de estrategias de armonización, documentación y orientación del proceso de armonización. Este papel debe ser desempeñado por una persona que está bien informado en la definición y modelado de procesos

PHM – Process Harmonization Manager: Gestor de Armonización de Procesos. Persona responsable de guiar la ejecución de las actividades del proceso de armonización. Este individuo debe poseer cualidades de gestión para que puedan: comprender la requisitos y necesidades de la organización, establecer prioridades y: obtener los recursos y elementos necesarios para la ejecución normal de las actividades.

SG – Steering Group: Grupo Directivo. Este grupo está formado por ejecutivos, o al menos un representante de las propuestas para aprobar recursos y / o cambios.

2.3.9.3. Productos de trabajo

Por último, los productos de trabajo definidos por HProcess son:

- Propuesta de armonización
- Estrategia de armonización
- Informe de aplicación de la estrategia de armonización
- Base de conocimiento.

Es preciso mencionar que para elaborar los productos de trabajo definidos en el proceso de armonización HProcess se emplea unas plantillas autónomas, que se encuentra en planteada en la sección de Apéndices de [22]. Estas plantillas tienen como propósito facilitar significativamente la elaboración de los productos, en aras de centrarse en los datos almacenados en su interior. Finalmente se precisa que los

productos de trabajo representan los resultados medibles de la aplicación del proceso de armonización HProcess.

2.3.10. Comparación de los métodos de armonización

Recordemos que los métodos de armonización son: el método de Homogenización HoMethod, el método de Comparación MaMethod, y el método de Integración IMethod. La Tabla V muestra una comparación entre estos tres métodos que soportan una armonización según lo establecido por HMethod.

TABLA V. Comparación de los métodos de Armonización

HoMethod	MaMethod	IMethod
Pone en armonía las diferentes estructuras de múltiples modelos y/o estándares gracias a una estructura común que disminuye la subjetividad. Permite establecer una comparación para identificar las similitudes y diferencias generales entre los procesos de los modelos a armonizar	Permite establecer una comparación uno a uno entre los elementos propios de cada modelo y/o estándar a armonizar, permitiendo asimilar elementos específicos. Esta parte es una comparación en mayor detalle que el establecido por HoMethod.	Pone en consonancia, unifica, une, ensambla, empalma las diferentes prácticas para poder emplear diferentes modelos. En este caso una práctica se realiza para dar cumplimiento a varios elementos (relacionados).

3. CAPITULO III. DESARROLLO Y RESULTADOS

3.1. TRABAJO DE CAMPO - PROCEDIMIENTO *INSCRIPCIONES Y ADMISIONES*.

El trabajo de campo se realizó con el propósito de poder determinar las características y necesidades de seguridad de la información del procedimiento *Inscripciones y Admisiones*, perteneciente a DARCA de la Universidad del Cauca. El trabajo de campo está estrechamente relacionado con las actividades (A1, A2, A3, A4) de HProcess. Además, se relaciona con los roles y productos de trabajo y los roles descritos en la sección 2.3.9.2. Para realizar el trabajo de campo se aplica la *Metodología de la Investigación, diseño y Ejecución* [19].

3.1.1. Técnicas e instrumentos de recolección de datos.

La Tabla VI muestra los instrumentos y técnicas de recolección de datos empleados con su respectiva técnica de registro de información.

Al aplicar encuestas y la lista de chequeo se generaron registros manuales que evidencian su diligenciamiento. Por otra parte, al aplicar las encuestas se generaron registros de voz. El ***Anexo B*** muestra las técnicas, instrumentos y los registros físicos generados.

TABLA VI. Técnicas e instrumentos de recolección de información.

Técnica de recolección de datos	Instrumento de recolección de datos	Técnica de Registro de información
Entrevistas	Cuestionario	Registro por otros medios: Grabaciones de voz
Encuestas	Cuestionario	Registro Manual: Hojas en físico
Listas de chequeo	Formulario	Registro Manual: Hojas en físico

Los instrumentos de recolección de datos fueron elaborados con base en los requisitos de la norma ISO 27001, en los objetivos de este trabajo de grado (enfocado a la fase *Ejecución* de un SGSI), y los resultados de la fase *Plan* de un SGSI.

Las preguntas fueron las mismas para todos los funcionarios. La elaboración de los cuestionarios se basó en el proceso ilustrado en la Fig. 13. Los cuestionarios se

realizaron a todos los funcionarios de DARCA, es decir que se tuvo en cuenta toda la población. Los cuestionarios requieren un lenguaje técnico, por lo tanto, fue indispensable hacer contacto con el entrevistado, y explicar cada una de las preguntas para un mejor desarrollo y recepción de los datos. Las encuestas y entrevistas fueron personales permitiendo la cooperación entre entrevistador y entrevistado. Finalmente, los cuestionarios de recolección de datos fueron elaborados con base en [87]–[90].

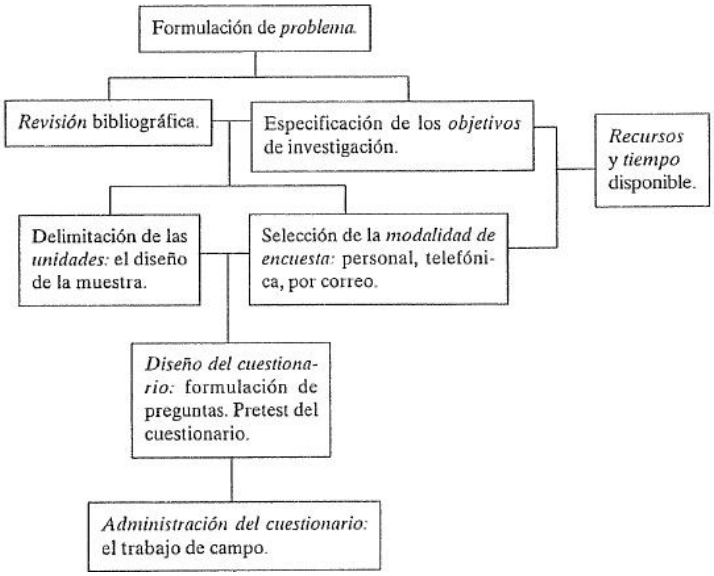

Fig. 13. Etapas para la elaboración de los cuestionarios. [91]

3.1.2. Encuestas

Se realizaron dos modelos de encuestas:

- Modelo de encuesta dirigido al jefe de DARCA
- Modelo de encuesta dirigido a los funcionarios de DARCA

3.1.2.1. Análisis e interpretación de encuesta dirigida al jefe de DARCA

- El jefe de DARCA manifiesta que su nivel de interés en el Sistema de Gestión de Seguridad de la Información es *Alto*.
- El jefe de DARCA manifiesta que tiene un nivel de interés *Alto* en que los funcionarios de DARCA reciban una capacitación básica en seguridad de la información
- El jefe de DARCA manifiesta que tiene un nivel de interés *Alto* en acoger la política de seguridad de la información para DARCA.

- El jefe de DARCA manifiesta que la hora más adecuada para realizar las capacitaciones es a las 11 AM o a las 5 PM.

El jefe de DARCA manifestó su apoyo y su alto interés en la implementación del SGSI en el procedimiento *Inscripciones y* Admisiones, lo cual beneficia a DARCA y el desarrollo del tercer objetivo específico de este trabajo de grado. Adicionalmente, manifestó el apoyo y alto interés en el establecimiento de la política de seguridad de la información y el programa de capacitación.

3.1.2.2. Análisis e interpretación de encuesta dirigida a funcionarios de DARCA

- Se pudo determinar que dos encuestados consideran que su nivel de conocimiento en seguridad de la información es de nivel “Alto”; seis consideran que es “Medio”; cinco consideran que es “Bajo”; y uno considera que es “Muy bajo”. Esto constituye una gran cantidad de funcionarios de DARCA que no tienen un nivel de conocimiento adecuado. Por lo tanto, se deben tomar las acciones pertinentes por parte de las directivas, teniendo en cuenta que los funcionarios que intervienen en el procedimiento *Inscripciones y Admisiones* manejan información de gran relevancia para la Universidad del Cauca.
- Se pudo determinar que cinco funcionarios encuestados consideran que su nivel de seguridad sobre los activos que manejan en su trabajo es “Alto”; cuatro consideran que es “Medio”; tres consideran que es “Bajo”; y dos consideran que es “Muy bajo”. Los funcionarios de DARCA reconocen que la información que manejan desde su puesto de trabajo debe ser altamente confidencial, por lo tanto, aunque algunos funcionarios no poseen abundantes conocimientos en seguridad de la información, si manifiestan tomar las acciones apropiadas sobre los activos de información. En consecuencia, se aplican estrategias de seguridad informales, siendo esto una gran vulnerabilidad teniendo en cuenta la importancia de la información que guardan los activos de información.
- Se pudo determinar que seis encuestados no saben de la existencia de un programa de capacitación en seguridad de la información en DARCA; cinco encuestados afirman que no existe; y tres encuestados manifiestan que si existe. La verdad es que el programa de capacitación en seguridad de la información no está formalmente establecido, según lo manifiesta el mismo Jefe de DARCA.
- Se pudo determinar que once de los funcionarios encuestados no han recibido ***ninguna*** capacitación el último año, en temas relacionados con la seguridad de la información. Por su parte solamente tres funcionarios manifiestan haber

recibido entre una y dos capacitaciones, sin embargo, manifiestan que han sido realizadas por instituciones externas a DARCA, por fuera de su trabajo. Los tres funcionarios que manifiestan haber recibido alguna capacitación en seguridad de la información encuentran que esto beneficia las prácticas en relación con el procedimiento *Inscripciones y Admisiones*.

- Se pudo determinar que doce funcionarios encuestados tienen un grado de interés *alto* en recibir capacitaciones acerca de la seguridad de la información. Por otra parte, dos encuestados manifiestan tener un grado de interés *medio*. Con esto se evidencia que se puede llevar a cabo una capacitación teniendo la disposición de los funcionarios que intervienen en el procedimiento *Inscripciones y Admisiones*.
- Se pudo determinar que cinco encuestados manifiestan que el horario más apropiado para realizar una capacitación es en las horas de la mañana; cinco de los encuestados manifiestan que en horas la tarde; tres encuestados manifiestan que después de las 6 PM; y un encuestado considera que debe hacerse en otro horario. Es importante que al realizar capacitaciones no se interfiera en las actividades laborales.
- Se pudo determinar que la totalidad de los encuestados manifiesta que no ha habido ningún incidente de seguridad de la información que haya sucedido en el procedimiento *Inscripciones y Admisiones* en el último año. Esto se debe a que se utilizan estrategias informales e indocumentadas para reportar incidentes de seguridad.
- Se pudo determinar que nueve de los encuestados no saben de la existe de una política de seguridad de la información para el procedimiento *Inscripciones y Admisiones*; cuatro encuestados manifiestan que si existe; y un encuestado manifiesta que efectivamente esta política no existe. Por lo tanto, se determina que esta política de seguridad de la información no se encuentra formalmente establecida. Algunos encuestados confunden estrategias con políticas de seguridad de la información.
- Se pudo determinar que el orden de importancia de los temas en seguridad de la información para los funcionarios de DARCA es el siguiente:

  Primero: Seguridad en la red

  Segundo: Seguridad del software

  Tercero: Seguridad de los documentos

  Cuarto: Seguridad del hardware

  Quinto: Seguridad de los empleados

3.1.3. Entrevistas

Se realizaron dos modelos de entrevistas:

- Modelo de entrevista dirigido al jefe de DARCA
- Modelo de entrevista dirigido a los funcionarios de DARCA

3.1.3.1. Análisis e interpretación de entrevista dirigida al jefe de DARCA

Políticas

- El jefe de DARCA manifiesta su apoyo en la implementación del SGSI en el procedimiento *Inscripciones y Admisiones* porque considera que es necesario e importante. También reconoce que no existe una política de seguridad de la información de aplicación para DARCA y que adicionalmente no conoce la política del sistema de gestión de seguridad de la información de la Universidad del Cauca. El jefe de DARCA no tiene claridad acerca de los procesos para aprobación y divulgación de políticas. Adicionalmente no sabe de procedimientos formales para hacer cumplir las políticas establecidas, expresando que esta tarea le corresponde al sistema de gestión de Calidad de la Universidad del Cauca.

- El jefe de DARCA manifiesta que en los dos años que se encuentra en este puesto de trabajo no se han presentado incidentes de seguridad de la información y que por lo tanto no ha sido necesario tomar ninguna acción frente a esto. Es importante destacar que el jefe de DARCA manifiesta que para garantizar la seguridad de la información lo único que se hace es darles recomendaciones generales a los funcionarios de DARCA acerca del cuidado de los equipos, recomendar especial atención a la seguridad de la información desde su puesto de trabajo y recalcar que no se permite el ingreso de personal no autorizado a las instalaciones de DARCA.

- El jefe de DARCA manifiesta que la restricción de control de acceso ante personal ajeno al departamento estaba controlada por una cerradura biométrica que actualmente no funciona, y que no ha sido posible hacerlo arreglar o cambiar, a pesar de las constantes solicitudes al departamento de mantenimiento, DivTIC y Vicerrectoría Académica.

- El jefe de DARCA manifiesta que no existe una política de seguridad de la información para DARCA y que no conoce la política existente para el procedimiento *Inscripciones y Admisiones.* También manifiesta que, sí se realiza

restricción de control de acceso al llevar a cabo el procedimiento *Inscripciones y Admisiones*, y que este control de acceso se lleva a cabo de manera continua.

- El jefe de DARCA manifiesta que todos los computadores de la división, y los computadores utilizados en el procedimiento *Inscripciones y Admisiones* se encuentran protegidos contra virus informáticos y que esta tarea es compartida con el área de mantenimiento.

- El jefe de DARCA manifiesta que para el procedimiento *Inscripciones y Admisiones* la División de las TIC proporciona unas copias de seguridad dos veces al día y que estas copias se realizan sobre el aplicativo utilizado.

- El jefe de DARCA manifiesta que las personas que intervienen en el procedimiento *Inscripciones y Admisiones* si establecen prácticas de seguridad para la selección y uso de contraseñas, y que estas contraseñas se cambian permanentemente cada mes. Además, expresa que los funcionarios que intervienen en procedimiento *Inscripciones y Admisiones* saben cómo utilizar los diferentes equipos de cómputo y aparatos tecnológicos para la seguridad del Hardware y del Software.

- El jefe de DARCA manifiesta que se revisan diariamente los derechos de acceso de los funcionarios que intervienen en el procedimiento *Inscripciones y Admisiones*, de manera que la sesión del aplicativo utilizado se cierra a las 6 de la tarde y en caso de necesitar más tiempo se solicita un permiso que se extiende hasta las 12 de la noche, momento en el cual se vuelve a cerrar la sesión.

- El jefe de DARCA manifiesta que no tiene conocimiento de las pruebas de calidad realizadas a las contraseñas, y finalmente expresa que existe un tiempo de inactividad para que los computadores suspendan la sesión en el sistema.

Capacitación

- El jefe de DARCA manifiesta que no existe un programa de capacitación de las políticas de seguridad de la información ni de temáticas relacionadas con la seguridad de la información, por lo tanto. Teniendo en cuenta lo anterior, es importante resaltar que DARCA tampoco cuenta con un procedimiento documentado de capacitación en seguridad de la información. Siguiendo este orden de ideas, los funcionarios de DARCA no conocen la normatividad relacionada con la seguridad de la información.

- El jefe de DARCA manifiesta que los funcionarios de DARCA no reciben una formación en seguridad de la información respecto a sus funciones de trabajo. Lo que se realiza es dictar unas directrices generales de seguridad relacionas con cambio de contraseñas, control de acceso y cifrado de la información digital.

- El jefe de DARCA manifiesta que el departamento no tiene contacto con grupos de interés, foros o profesionales en seguridad de la información y que tampoco se proporcionan boletines o socializaciones de los problemas de seguridad de los funcionarios de DARCA, y para terminar el jefe de DARCA considera que todos los temas de seguridad de la información son importantes y pertinentes.

Procedimientos y Registros

- El jefe de DARCA expresa no sabe de la ocurrencia de incidentes de seguridad de la información, y que no existe un procedimiento formalmente establecido para reportar los incidentes de seguridad en caso de llegar a suceder. Por otra parte, el jefe de DARCA expresa que las actividades como la actualización del antivirus es coordinada por el área de mantenimiento y que esto beneficia la seguridad de la información, sin embargo, dice que falta apoyo por parte de otras áreas como por ejemplo Gestión de la Calidad, Recurso Humanos y vicerrectoría Académica ya que DARCA depende mucho de ellos.

- El jefe de DARCA manifiesta que el mantenimiento preventivo de los computadores no se realiza de manera periódica por el área de mantenimiento. El jefe de DARCA también reconoce que ni DARCA ni el procedimiento *Inscripciones y Admisiones* realizan una revisión de las políticas, objetivos, controles, procesos, procedimientos y auditorias de seguridad de la información.

- El jefe de DARCA manifiesta que la documentación y registro de todo lo relacionado con la seguridad de la información no existe y que las principales vulnerabilidades que afectan la seguridad se deben a errores humanos.

3.1.3.2. Entrevistas realizadas a funcionarios de DARCA

- Se pudo determinar que doce entrevistados no conocen la política del sistema de gestión de seguridad de la información de la Universidad del Cauca; y dos entrevistados manifiestan si conocerla. Se evidencia que la gran mayoría de los funcionarios entrevistados no saben de la existencia de la política del Sistema de Gestión de Seguridad de la Información de la Universidad del Cauca, siendo este un documento de alto nivel que aplica en toda la institución y por lo tanto de

aplicabilidad en el procedimiento *Inscripciones y Admisiones*. Es realmente imprescindible que los funcionarios conozcan la política de seguridad de la información de la Universidad del Cauca la cual representa la posición del rector en cuanto a la implementación del SGSI, apoyo, generación y publicación de sus políticas, procedimientos e instructivos.

- Se pudo determinar que nueve entrevistados no saben cuál es el procedimiento para reportar los incidentes de seguridad de la información, y esto es porque el procedimiento no se encuentra establecido formalmente, según lo expreso el jefe de DARCA. Los otros cinco entrevistados hacen uso de maneras informales y no documentadas de reportar las fallas o incidentes de seguridad de la información.

- Todos los entrevistados manifiestan que su equipo de trabajo si se encuentra protegido contra virus. Lo correspondiente a la protección contra virus informativo es una labor que se comparte con el área de mantenimiento, según lo manifiestan los entrevistados. Además, expresan que se realizan actualizaciones de los programas antivirus con bastante regularidad y en consecuencia todos los equipos de trabajo empleados en el procedimiento *Inscripciones y Admisiones* cuentan con un programa antivirus actualizado.

- Diez de los entrevistados manifiestan que si almacenan información relevante para el procedimiento *Inscripciones y Admisiones* en el disco duro del equipo de trabajo. Por otra parte, cuatro de los funcionarios encuestados manifiestan que no. Al realizar la entrevista se pudo evidenciar que la mayoría de los entrevistados no tienen claridad de la información que se guarda en el disco duro y la información que se almacena en SIMCA. Los funcionarios almacenan actas, reportes y documentos en su equipo de trabajo, sin embargo, estos funcionarios no están acostumbrados a guardar copias de respaldo de manera frecuente.

- Tres funcionarios manifiestan que, si guardan copias de respaldo, pero no lo hacen regularmente o dicen no recordar cada cuanto lo hacen. Dos funcionarios dicen guardar copias de respaldo al final del periodo lectivo. Tres funcionarios expresan que guardan copias cada tres, dos y un mes. Finalmente, una de las personas encuestadas reconoce la importancia de las copias de respaldo y manifiesta hacerlo cada ocho días. Con esto se comprueba la gran necesidad de que el personal reciba capacitaciones en “contraseñas” de seguridad de la información. Adicionalmente, la necesidad de una política de contraseñas.

- Se pudo determinar que tres entrevistados no establecen prácticas de seguridad para la selección y uso de las contraseñas. Once de los entrevistados manifiestan tener algún tipo de práctica de seguridad para las contraseñas, Sin embargo, los funcionarios no tienen claridad acerca de cuáles son buenas prácticas de seguridad en el uso de contraseñas, ya que la mayoría de los funcionarios de DARCA no cambian con regularidad la contraseña de ingreso al equipo de trabajo o al aplicativo SIMCA.

- Se pudo determinar que uno de los entrevistados nunca ha cambiado la contraseña de ingreso al computador de trabajo. Dos entrevistados cambian la contraseña de ingreso al aplicativo SIMCA porque este lo solicita obligatoriamente. Uno de los entrevistados lo realiza cada año. Cuatro de los entrevistados cambian su contraseña cada dos o tres meses. Cuatro de los entrevistados lo hacen cada cinco o seis meses y tan solo uno de los entrevistados lo realiza cada mes. Por otra parte, dos entrevistados lo realizan cada ocho o quince días. Con esto se concluye que los funcionarios no establecen buenas prácticas de uso de contraseñas.

- Se puedo determinar que nueve de los entrevistados no sabe cómo utilizar su equipo de trabajo para la seguridad del Software y el Hardware, y cinco personas si lo saben. Este aspecto es de vital importancia ya que son los funcionarios los que más pueden aportar para la preservación y la seguridad de la información almacenada en los equipos de trabajo por medio de la protección del Hardware y el Software.

- Se pudo determinar que todos los entrevistados no han realizado capacitaciones en seguridad de la información suministrada por la Universidad del Cauca

- Se pudo determinar que tres entrevistados consideran importante los temas de “seguridad de los programas o aplicaciones”, cuatro de los entrevistados consideran que todos los temas son pertinentes. Otros temas pertinentes para los funcionarios son:

  Protección contra intrusos
  Control de acceso
  Resguardo de archivos para evitar accesos remotos
  Copias de respaldo
  Reporte de incidentes
  Que hacer en caso de un ataque informático
  Seguridad en la red

- Gran parte de los entrevistados no tienen claridad de los temas específicos en seguridad de la información de pertinencia para DARCA, por lo que consideran que ***todos*** los temas son pertinentes, sin embargo, existe una inclinación hacia temas como “copias de respaldo” y la “seguridad en la red”.

- Se pudo determinar que trece entrevistados no conocen sobre la normatividad relacionada con la seguridad de la información, y tan solo una persona reconoce que conoce sobre la norma NTC-ISO/IEC 27001.

3.1.4. Lista de chequeo

- La lista de chequeo indica que el procedimiento *Inscripciones y* Admisiones, perteneciente a DARCA solamente cumple con los requisitos correspondientes a la fase *Plan* del SGSI según lo establece la norma NTC-ISO/IEC 27001, lo cual se realizó gracias al proyecto [14] realizado por Juan Pablo Martinez y Diego Felipe Espinosa, con el apoyo del ingeniero Siler Amador Donado.

- El Sistema de Gestión de Seguridad de la Información necesita de acciones que provengan de la alta dirección de la Universidad del Cauca para que los esfuerzos realizados puedan tener continuidad.

- Gracias a la política de seguridad de la información de la Universidad del Cauca (aprobada bajo la resolución R-785 de 2015) se pueden realizar este y muchos más proyectos encaminados hacia la seguridad de la información, ya que existe el apoyo y el compromiso de la alta dirección de la Universidad del Cauca.

- Se pudo determinar que en el procedimiento *Inscripciones y Admisiones* existen prácticas de seguridad, estrategias y procedimientos de seguridad de la información que se llevan a cabo de manera informal y con poca regularidad.

- El procedimiento *Inscripciones y Admisiones* está incursionando en la implementación de un SGSI, y por lo tanto no cumplen con los requisitos de la fase *Ejecución* del SGSI establecidos en la norma NTC-ISO/IEC 27001.

3.1.5. Conclusiones

- El jefe de DARCA reconoce que una política de seguridad de la información para el procedimiento *Inscripciones y Admisiones* sería de gran utilidad para apoyar la aplicación de controles que disminuyan los riesgos de seguridad existentes.

Además, el jefe de DARCA manifiesta su apoyo en la implementación de esta política.

- Con la entrevista al jefe de DARCA se pudo deducir que el contenido de la política propuesta en la fase *Plan* del SGSI para el procedimiento *Inscripciones y Admisiones* sigue siendo pertinente.

- Se pudo determinar que las temáticas más apropiadas para una capacitación son aquellas que se relacionan con la política se seguridad de la información para el procedimiento *Inscripciones y Admisiones.*

- El control de acceso de personal ajeno a la división es de vital importancia, pero que ha sido muy difícil realizar este control debido a que los funcionarios no tienen una cultura de seguridad. Por lo tanto, se deduce que el control de acceso es algo indispensable en la política de seguridad de la información.

- En las entrevistas se pudo determinar que es indispensable se realicen las acciones pertinentes para la asignación de responsabilidades sobre los activos de información.

- Debido a la relación entre DARCA y la División de TIC (en cuanto a lo relacionado con las pruebas de seguridad de contraseñas, antivirus, suspensión de sesión en tiempos determinados en equipos y en SIMCA), es indispensable crear un camino de comunicación con estas áreas externas a DARCA para dar cumplimiento a esta parte de la política de seguridad de la información.

- Queda claro que no existe un programa de capacitación en seguridad de la información en DARCA y por lo tanto es muy difícil que los funcionarios de DARCA puedan conocer y relacionarse con diferentes temáticas, por ejemplo, la política del Sistema de Gestión de Seguridad de la Información de la Universidad del Cauca.

- Debido a la ausencia de capacitaciones en seguridad de la información en DARCA es evidente que no existen estrategias de formación ni un procedimiento documentado para realizar capacitaciones de seguridad de la información.

- Los funcionarios de DARCA no tienen una herramienta que les permita conocer la normatividad relacionada con la seguridad de la información en cuanto a sus funciones de trabajo. Es importante reconocer que la creación de boletines y actualizaciones periódicas relacionadas con los problemas de seguridad de la

información es una herramienta de apoyo en un programa de capacitación, y que sería de gran utilidad para DARCA.

- Se destaca que ni los funcionarios de DARCA ni los contratistas relacionados con el procedimiento *Inscripciones y Admisiones* han recibido una capacitación formal en seguridad de la información, pese a la importancia y sensibilidad de la información que manejan, y su gran importancia para la Universidad del Cauca.

- Lo concerniente a la seguridad de la información no es documentado, por lo que no existen registros de algún incidente sucedido en DARCA. Adicionalmente, no existe un procedimiento que defina el cómo debe ser reportados los incidentes en caso tal de que ocurran. Los procedimientos y registros de seguridad de la información que se necesitan deben ser establecidos.

- El SGSI es algo nuevo en DARCA, y no existen registros ni procedimientos de operación documentados. Por lo tanto, todos los procedimientos y registros especificados en la norma NTC-ISO/IEC 27001 hay que realizarlos para que el SGSI en el alcance del procedimiento *Inscripciones y Admisiones* se pueda operar.

De manera general se concluye que los funcionarios de DARCA no tienen las competencias suficientes para garantizar la confidencialidad, integridad y disponibilidad de la información que manejan, y en cualquier momento pueden presentarse incidentes de seguridad de la información. Por lo tanto, es indispensable que tanto el procedimiento *Inscripciones y Admisiones* complete la implantación del SGSI.

Teniendo en cuenta los hallazgos encontrados y las recomendaciones del jefe de DARCA y de los funcionarios, se llega a la conclusión general de que los controles de "Políticas[18]" y de "Concienciación o capacitación[19]" son los más pertinentes para ser llevados a cabo en la fase *Ejecución* del SGSI. A pesar de que DARCA requiere la implantación de otros controles, no se podrían abordar en este trabajo de grado debido a las limitaciones de recursos existentes, por eso en la sección de

[18] Control de seguridad "Políticas": Se refiere al control A.5.1.1: Políticas para la seguridad de la información, el cual se encuentra en el anexo A de la norma ISO/IEC 27001:2013.

[19] Control de seguridad "Concienciación": se refiere al control 7.2.2: Toma de conciencia, educación y formación en la seguridad de la información, el cual se encuentra en el anexo A de la norma ISO/IEC 27001:2013.

recomendaciones se plantean algunos controles para implementar en otro momento.

3.1.6. Controles de seguridad de la información para el procedimiento *Inscripciones y Admisiones*

Se realizó la selección de dos controles, sacados de la Declaración de Aplicabilidad – SOA ubicada en la tercera sección del ***Anexo A***. Después de varias reuniones con el jefe de DARCA de la Universidad del Cauca y de la exploración de las características y necesidades del procedimiento *Inscripciones y Admisiones,* anteriormente descrito se seleccionaron los controles se muestran en la Tabla VII. Estos dos controles se seleccionaron estratégicamente obedeciendo a las recomendaciones del jefe de DARCA.

- ✓ **Estados de un control de seguridad de la información**

La Fig. 14 muestra los diferentes estados en los que se puede fijar un control de seguridad de la información. Como se puede ver, existen cuatro estados: Estado ideal, Innecesario, Ausente, estricto e insuficiente.

Estado ausente: El control no se ha implementado aún, es decir que se ha identificado la necesidad de implementar un determinado control y se realizará por primera vez.

Estado insuficiente: El control se ha implementado de manera informal o se ha implementado de una manera muy elemental. Es necesario mejorar el control.

Estado ideal: Este estado es el que se debe garantizar. Consiste en que el control alcance el nivel de riesgo deseado.

Estado estricto: El control se ha implementado superando levemente el nivel de riesgo deseado.

Estado innecesario: El control se ha implementado superando las expectativas y el nivel de riesgo deseado. En este punto el control se ha optimizado, y por lo tanto no es necesario realizar mejoras ni acciones preventivas /correctivas.

Determinar el estado de un control sirve para medir y comparar un estado inicial (estado antes de implementar un control) con un es estado final (después de implementar un control).

TABLA VII. Controles fase *Ejecución* del SGSI para el procedimiento *Inscripciones y Admisiones*

	Control Seleccionado	Razón/Justificación de la Selección
Dominio	**A.5** Políticas de seguridad de la información	
Objetivo de Control	**A.5.1** Orientación de la dirección para la gestión de la seguridad de la información. Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos de DARCA, con la legislación y reglamentación pertinentes.	
Control 1	**A.5.1.1 Políticas para la seguridad de la información** La dirección debería definir, aprobar y publicar un conjunto de políticas para la seguridad de la información; y comunicar las políticas a los empleados de DARCA y a las partes externas pertinentes.	– En DARCA no existen políticas para la seguridad de la información específicas a sus necesidades. – La política de seguridad de la información en DARCA es la base para dar cumplimiento a otros controles especificados en el SOA. – En DARCA no se conoce ni se implementa la política de la seguridad de la información de la Universidad del Cauca
Dominio	**A.7** Seguridad de los recursos humanos	
Objetivo de Control	**A.7.2** Durante la ejecución del empleo. Asegurarse de que los empleados y contratistas tomen conciencia de las responsabilidades de seguridad de la información	
Control 4	**A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información** Todos los empleados de DARCA y en donde sea relevante deberían recibir un entrenamiento adecuado y actualizaciones regulares sobre las políticas y procedimientos de la Universidad del Cauca que sean relevantes para las funciones de su cargo.	• Resultados de la gestión del Riesgo • Los empleados de DARCA carecen de conocimientos suficientes en seguridad de la información.

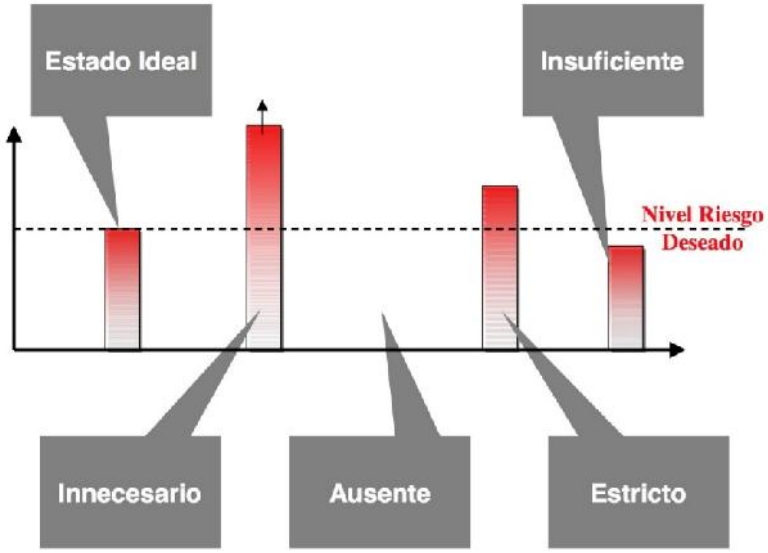

Fig. 14. Estado de un control. [92]

TABLA VIII. Actividades de Mitigación para el procedimiento *Inscripciones y Admisiones*

A.5.1.1 Control: Políticas para la seguridad de la información	
Área de Seguridad	**Actividades de Mitigación**
Políticas y Reglamentos de Seguridad	Documentar formalmente las políticas relacionadas con la seguridad del procedimiento *Inscripciones y Admisiones*.
A.7.2.2 Control: Toma de conciencia, educación y formación en la seguridad de la información	
Área de Seguridad	**Actividades de Mitigación**
Conciencia de Seguridad y Formación	Elaborar una estrategia de capacitación documentada que incluya concienciación sobre la seguridad y la formación relacionada con la seguridad para las tecnologías compatibles en el procedimiento *Inscripciones y Admisiones*.
	Elaborar un plan de capacitación en seguridad para las tecnologías soportadas en el procedimiento *Inscripciones y Admisiones*.
	Diseñar un mecanismo formal para proporcionar a los miembros del personal con actualizaciones periódicas / boletines sobre los problemas de seguridad importantes sobre el procedimiento *Inscripciones y Admisiones*.

- ✓ **Plan de mitigación de riesgos**

Cada control seleccionado tiene asociadas unas Actividades de Mitigación sacadas de los planes de tratamiento de riesgo, pero en este proyecto de investigación no se pueden abordar todas porque el costo sería muy elevado y adicionalmente el tiempo disponible se incrementaría. Por esta razón se seleccionaron las Actividades de Mitigación que muestran la Tabla VIII. La selección de controles y actividades de mitigación se realizó con el acompañamiento del jefe de DARCA de la Universidad del Cauca. Las actividades escogidas requieren de una inversión considerable de recursos y son de muchísima utilidad para procedimiento *Inscripciones y Admisiones*, siendo esto de gran beneficio para DARCA.

3.2. ARMONIZACIÓN DEL MODELO EFQM CON ISO/IEC 27001

La armonización entre el modelo EFQM:2013 y la norma ISO/IEC 27001:2013 se realizó con base en el método HProcess descrito en la sección 2.3.9. La armonización realizada consistió básicamente, en adecuar el proceso HProcess al caso particular de este trabajo de grado. En este sentido, el proceso de armonización [22] (pp.128-140) presenta las siguientes unidades de análisis:

- Las actividades de HProcess
- Estrategia de armonización
- La armonización de los modelos.

3.2.1. Actividades de HProcess para la armonización de ISO/IEC 27001 y EFQM.

La Fig. 12 muestra el proceso efectuado para la armonización entre modelo EFQM y la norma ISO/IEC 27001. A continuación, se presenta una descripción de las actividades de HProcess con sus respectivos productos de trabajo.

- ✓ **Actividad 1. Puesta en marcha.**

Para comenzar se asignaron los roles definidos en HProcess, de manera que intervinieron un total de cuatro personas entre las cuales se repartieron los roles y se establecieron las correspondientes responsabilidades.

PHM – Gestión del proceso de Armonización: Dos estudiantes, investigadores del presente trabajo de grado.

PE – Ingeniero de Procesos: Estudiante investigador

P – Ejecutante: Jefe de DARCA, responsable del procedimiento *Inscripciones y Admisiones.*

SG – Grupo Directivo: Por una parte, el jefe de DARCA, responsable del procedimiento *Inscripciones y Admisiones,* y por otra parte el ingeniero director del presente trabajo de grado

R – Revisor: Labor que desempeña el ingeniero de procesos, director de este trabajo de grado.

Adicional a la asignación de roles, se identifican las necesidades de armonización, los objetivos de armonización, entre otros, tal como lo refiere la *propuesta de armonización* en la Tabla IX. Como resultado de la actividad "Puesta en Marcha" se obtuvo el producto de trabajo denominado *Propuesta de Armonización*[20].

La elección de la norma ISO/IEC 27001 se realizó con base a las características y necesidades de seguridad de la información del procedimiento *Inscripciones y Admisiones*, perteneciente a DARCA de la Universidad del Cauca, tal como lo corrobora el trabajo de campo de la sección 3.1. El modelo EFQM, por su parte, se seleccionó con base en las explicaciones dadas en la sección 2.1.1, para apoyar el cumplimiento de los procesos descritos en ISO/IEC 27001. Así pues, el objetivo final de la actividad 1 se centra en definir una propuesta para la integración de las prácticas del modelo EFQM y de la norma ISO 27001.

- ✓ **Actividad 2. Análisis y definición**

En la segunda actividad se realizó la estrategia de armonización HStrategy, la cual se compone de un conjunto de métodos que permitirán finalmente adaptar el modelo EFQM y la norma ISO/IEC 27001: 2013, de acuerdo a las necesidades de armonización de la organización. Los métodos de armonización incluidos en HStrategy fueron homogeneización, comparación e integración de prácticas. Adicionalmente se estableció la direccionalidad de la armonización, siendo la norma ISO/IEC 27001 la columna vertebral.

[20] Propuesta de armonización: Es un producto de trabajo al cual se le da cumplimiento empleando la plantilla proporcionada por C. Pardo en [63] (p.131) y [22] (pp-199-206).

TABLA IX. Síntesis de la propuesta de armonización

Plantilla: Propuesta de proyecto de armonización		
Objetivo:		
Proyecto de armonización		
Primer nombre	Procedimiento *Inscripciones y Admisiones*	
Nombre del Proyecto de armonización	Adaptación de un marco de referencia con base en la norma ISO/IEC 27001:2013 y el modelo EFQM	
Nombre de la persona a cargo del caso de estudio	Dokia Marisol Zúñiga Mosquera	
Nombre de la persona que representa	Deisy Francely Imbachi – Fabio Hernán Cerón	
Objetivos y Alcance del proyecto de Armonización		
Necesidades de negocio	Disponer de un marco de referencia de aplicación general para la implementación de un SGSI con base en los requisitos de la norma ISO/IEC 27001. El modelo EFQM:2013 se elige por tener un alto nivel de abstracción y se propone su empleo sirviendo como apoyo a los requisitos de la norma ISO/IEC 27001:2013. La combinación de ellos debería emplearse para mejorar los procesos de implementación de un SGSI (Sistema de Gestión de Seguridad de la Información).	
Objetivos generales de armonización	Integrar un modelo de referencia para la implementación de un SGSI en el procedimiento *Inscripciones y* Admisiones, perteneciente a DARCA de la Universidad del Cauca, tomando como eje fundamental a la norma ISO/IEC 27001 e incorporando en ellos los principios del modelo EFQM que apoyan en su implementación.	
Alcance del proyecto de armonización	Armonizar/adaptar los principios establecidos por el modelo EFQM con la norma ISO/IEC 27001.	
Proceso de Armonización	El proceso de armonización a seguir es el descrito en ARMONÍAS (Proceso para realizar una armonización de múltiples modelos [61]).	
Modelos a analizar y área o proceso que es objeto de estudio		
Modelo A: Modelo base para llevar a cabo la armonización con respecto a otros modelos	ISO/IEC 27001 EFQM	Procesos relacionados con el cumplimiento de los requisitos de un SGSI establecidos por la norma ISO 27001
Recursos e infraestructura de trabajo		
ARMONÍAS Asesor de Proyectos- APA	2 Personas	
Ingeniero de Procesos - PE	1	
Ejecutante - P	1	
Grupo Directivo - SG	1	
Descripción general de la planeación del proyecto de armonización		

CRONOGRAMA: Se presenta la visión general del plan general de armonización en la organización.

Meses y Semanas / **Actividades**	Mes 1				Mes 2				Mes 3				Mes n			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Inicio	X	X	X													
Análisis y Definición			X	X	X											
Ejecución						X	X	X								
Comprobar									X	X	X					

El modelo A constituye la adaptación entre en modelo EFQM y la norma ISO/IEC 27001, y solo tiene una iteración. Mas iteraciones pueden llevarse a cabo a partir de recomendaciones o prácticas que se necesiten adicionar al modelo A.

La estrategia de armonización se muestra en la sección 3.2.2 con mayor detalle. La estrategia fue descrita por el Ingeniero de Proceso (PE). Luego, se estableció un proceso de búsqueda para descubrir casos de armonización anteriores, y en este sentido, no se obtuvo ningún caso de armonización anterior. Como resultado de la actividad "Análisis y definición" se obtuvo el producto de trabajo denominado *Estrategia de Armonización*[21].

- ✓ **Actividad 3. Ejecución**

La tercera actividad consistió en llevar a cabo los diferentes modelos establecidos en la estrategia de armonización HStrategy. Los roles encargados de ejecutar la estrategia fueron PHM, y PE.

La información relativa a la ejecución de la HStrategy se registró en un *Informe de Aplicación de la Estrategia de Armonización*, el cual constituye el producto de trabajo que resulta de la actividad *Ejecución*. En la sección 3.2.3 hasta 3.2.5 se presenta una descripción detallada de la ejecución de la estrategia de armonización para obtener la adaptación entre el modelo EFQM y la norma ISO/IEC 27001. Finalmente se redactaron las lecciones aprendidas, las cuales se muestran en sección 3.2.6.

- ✓ **Actividad 4. Revisión**

En la cuarta actividad se realizó una exploración y análisis de los resultados obtenidos en todo el proceso de armonización. En este aspecto se redactaron las correspondientes observaciones y reflexiones que sirven como la base de conocimiento para futuros proyectos de armonización.

3.2.2. Estrategia de Armonización HStrategy para la armonización de ISO/IEC 27001 y EFQM.

La estrategia de armonización empleada para la adaptación de la norma ISO/IEC 27001 con el modelo EFQM se compone de tres métodos: Homogenización – ***HoMethod***, Comparación – ***MaMethod***, Integración – ***IMethod***. Esta estrategia se ilustra en la Fig. 15, y facilita el proceso de armonización de modelos múltiples reduciendo la subjetividad, a la vez que facilita la gestión de las actividades. Esta

[21] HStrategy consistió en describir las actividades a realizar con la plantilla CSPE (Estructura Común de Elementos de Proceso), proporcionada por C. Pardo en [63].

estrategia se ha desarrollado con base en las necesidades identificadas en el procedimiento inscripciones y admisiones.

La Fig.15 ilustra que la estrategia comienza con la homogenización de los modelos, luego pasa a una comparación entre ellos y finalmente se realiza la integración. En este sentido es preciso aclarar que el modelo de homogenización y comparación definen los lineamientos para realizar una posterior integración/adaptación, por lo tanto, al ejecutar los dos primeros modelos se da cumplimiento al primer objetivo específico de este trabajo de grado. Luego al ejecutar el modelo de integración, se da cumplimiento al segundo objetivo específico.

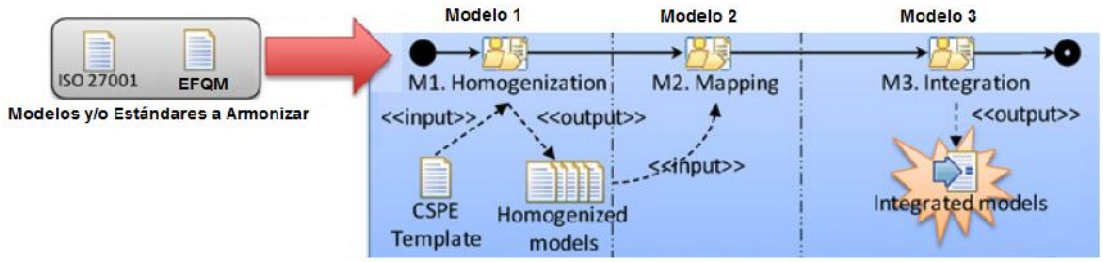

Fig. 15. Producto de Trabajo No.2: Métodos que componen la estrategia de armonización.

3.2.3. Homogenización de ISO 27001 y EFQM

La ejecución de la estrategia de armonización inicia con la homogenización de la norma ISO/IEC 27001 y del modelo EFQM, en aras de poder establecer una base común que permita comparar uno a uno los elementos de proceso de cada uno de ellos. Para realizar la homogenización se emplea la CSPE (Estructura Común de Elementos de Proceso[22]).

La homogenización permitió identificar los elementos comunes de ISO 27001 y EFQM a un alto nivel, con lo que fue posible analizar la complejidad, las similitudes y las diferencias existentes entre ellos. Así pues, también se pudo llevar a cabo un análisis en profundidad de los elementos constitutivos de los modelos involucrados. La Tabla X ilustra la homogenización de la norma ISO 27001 y EFQM en donde se ha empleado la plantilla propuesta por C. Pardo en [22] (p.108)

[22] CSPE - Estructura Común de Elementos de Proceso, definida por C. Pardo en [22]

TABLA X. Homogenización de modelos a alto nivel usando CSPE.

Sección	Estereotipos o elementos	Modelo EFQM	ISO/IEC 27001
Sección 1: Descripción (SD)	SD1. Categoría de proceso	X	X
	SD2. Procesos	X	X
	SD3. Actividades	X	
	SD4. Tareas	X	
Sección 2: Roles y Recursos (SRR)	SRR1. Roles	X	X
	SRR2. Herramientas		
Sección 3: Control (SC)	SC1. Artefactos	X	
	SC2. Objetivos	X	X
	SC3. Métricas	X	
Sección 4: Información Adicional (SIA)	SIA1. Procesos relacionados	X	
	SIA2. Métodos		

3.2.4. Comparación de ISO 27001 y EFQM

Paso seguido en la estrategia de armonización se procede a realizar la comparación entre el modelo EFQM y la norma ISO/IEC 27001. La comparación se realizó con respecto a un análisis comparativo, estableciendo relaciones entre los elementos constitutivos de cada marco de referencia. La direccionalidad de la comparación fue establecida tomando como punto de referencia a la norma ISO/IEC 27001:2013. Así pues, se procedió a comparar el modelo EFQM con respecto a la norma ISO 27001, tal como lo ilustra la Tabla XI. Esta direccionalidad se eligió con el propósito de poder apuntar en un futuro, hacia una posible certificación de la norma ISO 27001 en el procedimiento *Inscripciones y Admisiones*, de DARCA de la Universidad del Cauca. Par realizar la comparación fue necesario realizar un mapeo entre la norma y el modelo, el cual se muestra en el ***Anexo C***.

TABLA XI. Correspondencia y cobertura encontradas entre ISO 27001 y EFQM

Grupo de Procesos de ISO/IEC 27001	Procesos de ISO27001	Procesos de modelo EFQM
PG1. 4 Contexto de la organización	P1. 4.1. Conocimiento de la organización y de su contexto	P1. Estrategia
	P2. 4.2. Necesidades y expectativas de las partes interesadas	P1. Estrategia
	P3. 4.3. Alcance del SGSI	P1. Estrategia
	P4. 4.4. SGSI	NA

Grupo de Procesos de ISO/IEC 27001	Procesos de ISO27001	Procesos de modelo EFQM
PG2. 5 Liderazgo	P1. 5.1 Liderazgo y Compromiso	P1. Liderazgo
	P2. 5.2. Política	P1. Liderazgo
	P3. 5.3. Roles, responsabilidades en la organización	P1. Liderazgo
PG3. 6 Planificación	P1. 6.1. Acciones para tratar riesgos y oportunidades	P1. Estrategia
	P2. 6.2. Objetivos de la seguridad de la información y planes para lograrlos	P1. Estrategia
PG4. 7 Soporte	7.1. Recursos	P1. Alianzas y Recursos
	7.2. Competencia	P1. Personas
	7.3. Toma de conciencia	P1. Personas
	7.4. Comunicación	P1. Alianzas
	7.5. Información Documentada	P1. Procesos, productos y servicios
PG5. 8 Operación	8.1. Planificación y control operacional	P1. Procesos, productos y servicios P2. Estrategia
	8.2. Valoración de riesgos de la seguridad de la información	P1. Estrategia
	8.3. Tratamiento de riesgos de la seguridad de la información	P1. Estrategia
PG6. 9 Evaluación de desempeño	9.1. Seguimiento, medición, análisis, evaluación	P1. Resultados en personas P2. Resultados en clientes P3. Resultados en la sociedad
	9.2. Auditoria interna	P1. Resultados clave del negocio
	9.3. Revisión por la dirección	P1. Resultados clave del negocio
PG7. 10 Mejora	10.1. No conformidades y acciones correctivas	P1. Resultados clave
	10.2. Mejora Continua	P1. Liderazgo. P2. Estrategia P3. Personas P4. Recursos y alianzas P5. Procesos, productos y servicios P6. Resultados clave de negocio

3.2.5. Integración de ISO 27001 y EFQM

La integración entre la norma ISO/IEC 27001 y el modelo EFQM se realizó tomando únicamente las cláusulas de la norma ISO 27001 que corresponden a la fase *Ejecución* de un SGSI. Esto se realizó de acuerdo a los objetivos planteados en este trabajo de grado, sin embargo, para futuros proyectos se pueden tomar otras cláusulas.

TABLA XII. Estructura de modelo unificado

Clausulas		**Actividades**
		Gestión de la Calidad Total
CL5	Clausula 5.1	Criterio 1
CL 6	Clausula 6.2	Criterio 2.
CL 7	Clausula 7.1	Criterio 4
	Clausula 7.2	Criterio 3
	Clausula 7.3	Criterio 3
	Cláusula 7.5	Criterio 5
CL 8	Clausula 8.1	Criterio 5.
ISO/IEC 27001:2013		Modelo EFQM

3.2.6. Lecciones aprendidas

Esta sección expone los beneficios, las limitaciones y las lecciones aprendidas al llevar a cabo la armonización entre modelo EFQM y la norma ISO/IEC 27001. En este sentido, es preciso destacar que la comunicación con la organización (en este caso, con el jefe de DARCA) fue indispensable al momento de establecer un marco de referencia que efectivamente sea de utilidad para las necesidades de la organización.

Fue necesario realizar reuniones semanales entre las personas que desempeñaban algún rol dentro del proceso HProcess para discutir temas relacionados con el proceso de armonización.

Adicionalmente, fue necesario que los investigadores buscaran por su cuenta las herramientas necesarias que les permitieran adquirir conocimientos en las diversas temáticas involucradas en este trabajo de grado, ya que no se disponían de los recursos económicos suficientes para adquirir un entrenamiento formal, o una certificación en el modelo EFQM, norma ISO 27001, modelos y demás elementos esenciales para realizar una armonización de modelos múltiples.

3.3. ALCANCE DEL PROCEDIMIENTO *INSCRIPCIONES Y ADMISIONES*

Es preciso aclarar que este trabajo de grado constituye una iniciativa por parte de dos estudiantes de la FIET[23] para contribuir en el mejoramiento de la seguridad de la información del procedimiento *Inscripciones y* Admisiones, por lo tanto, las acciones tomadas por parte de los estudiantes no constituyen una medida reglamentaria de la alta dirección de la Universidad del Cauca (en este caso, el rector y su equipo directivo). Debido a esto, y basándose en las propias experiencias vividas en DARCA, los estudiantes no cuentan con el apoyo suficiente para ser involucrados en todas las actividades que se realizan en el procedimiento *Inscripciones y Admisiones*. En este punto es preciso decir que las actividades que componen el procedimiento *Inscripciones y Admisiones* se llevan a cabo en el trascurso de un semestre, y que involucran una gran cantidad de elementos y actores que se salen del alcance estipulado en este proyecto.

A razón de lo expuesto anteriormente, y teniendo en cuenta que el alcance de este proyecto se enfoca en la División de Admisiones, Registro y Control Académico de la Universidad del Cauca, es decir DARCA, se sale de nuestras manos tener acceso a otras entidades como UDEA[24], la cual es un agente externo a la Universidad que interviene en el procedimiento *Inscripciones y Admisiones*, según lo muestra la Fig. 6. En este sentido, la fase *Ejecución* del SGSI en el procedimiento *Inscripciones y Admisiones* abarca únicamente a DARCA y a los controles seleccionados descritos en la sección 3.1.6.

Luego de realizar la armonización entre el modelo EFQM y la norma ISO/IEC 27001:2013 se procede a exponer el marco de referencia propuesto, ante el personal que interviene en el procedimiento *Inscripciones y Admisiones*, el cual denominaremos "*Equipo de funcionarios de DARCA*". Así pues, se presentó al *equipo de DARCA* la propuesta para realizar la fase *Ejecución* del SGSI en el procedimiento *Inscripciones y Admisiones*. Luego, la propuesta presentada fue analizada por el *equipo de DARCA*, en compañía de los estudiantes de este trabajo de grado, con el propósito de poder evaluar cómo esta propuesta beneficiaría a DARCA. En este análisis realizado por el equipo DARCA se encontró que existen necesidades de seguridad de la información a las que se debe prestar mayor interés debido a su criticidad e importancia para el cumplimiento de los objetivos

[23] FIET: Facultad de Ingeniería Electrónica y Telecomunicaciones de la universidad del Cauca

[24] UDEA - Universidad de Antioquia: Proveedor de servicios que realiza la lectura de las hojas de respuesta de la prueba de Admisión.

estratégicos de la Universidad del Cauca. En este sentido, se presentó mayor interés hacia las tareas que componen la *Evaluación de la Prueba,* ya que algún incidente de seguridad de la información en esta parte implicaría medidas legales de gran magnitud. Finalmente, el equipo DARCA decidió que la solución planteada fuera enfocada hacia la *Evaluación de la Prueba.* Es por esto que, aunque el tercer objetivo específico de este trabajo de grado estuvo orientado inicialmente hacia el procedimiento *Inscripciones y Admisiones*, fue necesario orientarse hacia los aspectos más importantes de este procedimiento*.* Finalmente se destaca que gracias al trabajo realizado en el marco de este trabajo de grado se logró impactar positivamente sobre las actividades pertenecientes al procedimiento *Inscripciones y Admisiones*. Todo esto se debe a que las actividades que componen el procedimiento *Inscripciones y Admisiones,* mostrados en la Fig. 6 se relacionan y se engranan de manera que las acciones realizadas en una actividad afectan a las demás.

3.4. IMPLANTACIÓN DE LA FASE *EJECUCIÓN* DEL SGSI

Este capítulo está dedicado a describir la aplicación del marco de referencia propuesto para la implantación de la fase *Ejecución* de un SGSI en el alcance del procedimiento *Inscripciones y* Admisiones, perteneciente a DARCA de la Universidad del Cauca. La aplicación del marco de referencia propuesto corresponde a la tercera fase de la estrategia de investigación, es decir, la *solución de problemas* de la *Investigación-Acción* presentada en la sección 1.3 de este documento.

El marco de referencia propuesto constituye la solución planteada para realizar la fase *Ejecución* del SGSI. En este sentido es importante recordar que la fase *Ejecución* del SGSI no incluye todas las cláusulas de la norma ISO/IEC 27001. Esto se debe a que la fase *Plan* del SGSI ya se ha desarrollado en el procedimiento *Inscripciones y Admisiones*, y que la fase *Verificar* del SGSI contiene elementos de auditoria y revisión que no se abordan en este trabajo de grado.

Así pues, se retoma la descripción de los documentos obligatorios ilustrados en la Fig. 7, correspondientes a la fase *Ejecución* del SGSI. Estos documentos obligatorios constituyen la evidencia del cumplimiento de las cláusulas de la norma ISO/IEC 27001. Es preciso recordar que los documentos obligatorios que le corresponden a la fase *Ejecución* del SGSI son:

- Planes de Ejecución
- Documentación de Controles

- Artefactos operacionales

Para obtener estos documentos se definieron cuatro fases que se ilustran en la Fig.16, que definen el camino para implementar la fase *Ejecución* del SGSI de acuerdo a los elementos que brinda el modelo EFQM para el marco de referencia propuesto, en beneficio del cumplimiento de los requisitos de la norma ISO/IEC 27001:2013. Estas fases son:

- Fase 1. Compromisos de la alta dirección
- Fase 2. Autoevaluación del cumplimiento de las cláusulas de Fase *Ejecución* del SGSI.
- Fase 3. Elaboración y despliegue de Planes de acción para el cumplimiento de las cláusulas de la Fase *Ejecución* del SGSI.
- Fase 4. Validación de los resultados

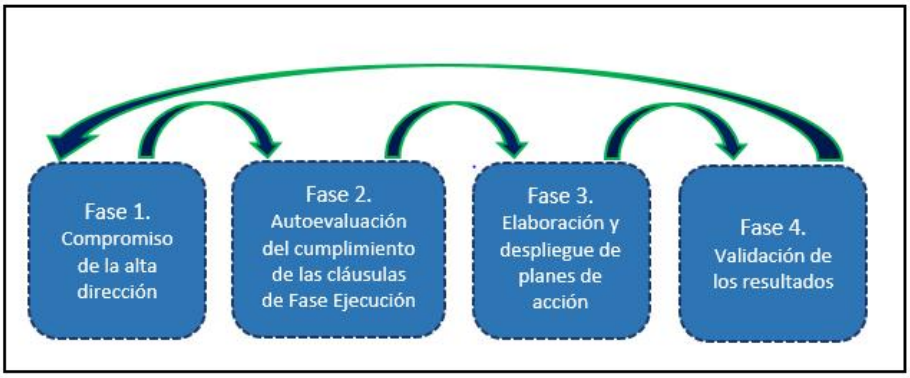

Fig. 16. Etapas de implementación de la fase *Ejecución* del SGSI

3.4.1. Fase 1. Compromisos de la alta dirección.

3.4.1.1. Descripción de la Fase 1.

La primera fase constituye la clave del éxito en el desarrollo de la fase *Ejecución* del SGSI. Cuando la alta dirección se compromete con la implementación del sistema de gestión de seguridad de la información, se pueden desarrollar cualquiera de las etapas del ciclo PHVA para el SGSI.

Para realizar esta fase se siguieron los siguientes pasos:

- Dar a conocer el proyecto de SGSI (para el procedimiento *Inscripciones y Admisiones*) a la alta dirección.
- Desarrollar compromisos por parte de la alta dirección.

La Tabla XIII presenta el objetivo, actividades, indicador y producto de trabajo correspondiente a la primera fase para la implementación de la fase *Ejecución* del SGSI.

TABLA XIII. Descripción de la primera fase para la implementación de la fase *Ejecución*

<table>
<tr><th colspan="2">Compromisos de la alta dirección</th></tr>
<tr><td colspan="2">Objetivo: Conseguir que el jefe de DARCA se comprometan con el desarrollo de la fase Ejecución del SGSI en el alcance del procedimiento Inscripciones y Admisiones.</td></tr>
<tr><th>Actividades</th><th>Indicador</th></tr>
<tr><td>– Realizar reuniones con el jefe DARCA para dar a conocer la importancia de un SGSI y los requisitos de la norma ISO/IEC 27001.
– Realizar reuniones para dar a conocer la fase Plan del SGSI finalizada en el procedimiento Inscripciones y Admisiones.
– Realizar reuniones para dar a conocer la fase Ejecución del SGSI a desarrollar en el procedimiento Inscripciones y Admisiones.
– Adquisición de compromisos por parte del jefe DARCA</td><td>– El jefe de DARCA se compromete con la fase Ejecución del SGSI en el procedimiento Inscripciones y Admisiones</td></tr>
<tr><td colspan="2">– Producto de trabajo: Acta de compromiso del jefe DARCA con el desarrollo de la fase Ejecución del SGSI.</td></tr>
</table>

Desarrollo de la Fase 1.

En esta fase se llevaron a cabo las siguientes actividades:

- La primera fase inició con una reunión realizada en las instalaciones de la División de Admisiones, Registro y Control – DARCA, en donde participaron los estudiantes Fabio Cerón y Deisy Imbachi, con la presencia del jefe de DARCA. En esta primera reunión se le dio a conocer al jefe de DARCA el contexto en que se encuentra ubicado este trabajo de grado y los beneficios en cuanto al mejoramiento de la seguridad de la información en el procedimiento *Inscripciones y Admisiones.*

- En una segunda reunión se dieron a conocer los aspectos más relevantes de un SGSI y la importancia de su implantación para la preservación de la confidencialidad, integridad y disponibilidad del procedimiento *Inscripciones y Admisiones*. Además, se realizó una introducción a la norma ISO/IEC 27001 y sus requisitos con base en las fases del ciclo Deming.

- En una tercera reunión se realizó una descripción de la fase *Plan* del SGSI y de los documentos obligatorios que están contenidos en esta fase, desarrollada y finalizada para el procedimiento *Inscripciones y Admisiones.*

- En una cuarta reunión se realizó una descripción de la fase *Ejecución* del SGSI y de los documentos obligatorios y actividades respecto a esta fase, la cual se desarrolla en el alcance del procedimiento *Inscripciones y Admisiones*.

- Finalmente, en una quinta reunión se determinaron los compromisos por parte del jefe de DARCA para desarrollar la fase *Ejecución* del SGSI en el procedimiento *Inscripciones y Admisiones.*

3.4.1.2. Productos de trabajo de la Fase 1.

Los registros de las actas de las reuniones realizadas se muestran en el ***Anexo D***. La ultima acta muestra los compromisos adquiridos por el jefe de DARCA con respecto a la fase *Ejecución* del SGSI en el alcance del procedimiento *Inscripciones y Admisiones.*

3.4.2. Fase 2. Autoevaluación del cumplimiento de las cláusulas de Fase Ejecución del SGSI.

3.4.2.1. Descripción de la Fase 2.

La segunda fase consiste en evaluar los criterios del marco de referencia propuesto (utilizando el *Explorador de oportunidades*) en el alcance del procedimiento *Inscripciones y Admisiones*. Con el desarrollo de esta fase se obtiene una visión general del estado de la seguridad de la información (con respecto a la fase *Ejecución* del SGSI) en el procedimiento *Inscripciones y Admisiones*. Los datos resultantes permitirán establecer las áreas de mejora y puntos fuertes de la seguridad de la información.

La Tabla XIV presenta el objetivo, actividades, indicador y producto de trabajo correspondiente a la segunda fase.

TABLA XIV. Descripción de la segunda fase del marco de referencia propuesto

Autoevaluación	
Objetivo: Realizar el proceso de autoevaluación para el procedimiento *Inscripciones y Admisiones*, lo cual se emplea como herramienta sistemática para mostrar el rendimiento de la organización. Los resultados obtenidos se utilizan para desarrollo de planes de acción.	
Actividades	**Indicador**
– Asignar un responsable al desarrollo del proceso de autoevaluación. – Desarrollo y registro de los cuestionarios "explorador de oportunidades" para cada uno de los criterios y subcriterios del marco de referencia propuesto. – Procesamiento y Análisis de los cuestionarios. – Conclusiones de los cuestionarios (Se identifican puntos fuertes, que se deben potenciar o áreas de mejora sobre, sobre las cuales se debe actuar)	– Autoevaluación finalizada obteniendo una comprensión de la situación real de la organización.
Producto de trabajo: Informe de evaluación y diagnóstico de la autoevaluación.	

3.4.2.2. Desarrollo de la Fase 2.

La autoevaluación se realiza para verificar el cumplimiento de las cláusulas correspondientes a la fase *Ejecución* del SGSI, según la norma ISO/IEC 27001:2013. El cuestionario de autoevaluación de seguridad de la información empleado se muestra en el ***Anexo E***.

Esta fase implica cuatro actividades que fueron desarrolladas de la siguiente manera:

- Las personas encargadas de realizar la autoevaluación fueron los estudiantes Deisy Imbachi y Fabio Cerón, sin embargo, una vez finalizado este trabajo de grado se pueden designar a otras personas.

- Se aplicaron cuestionarios según los criterios y subcriterios del modelo EFQM que benefician el cumplimiento de las cláusulas de la fase *Ejecución* de un SGSI, según la norma ISO 27001.

- Se realiza el procesamiento, análisis e interpretación de los datos recolectados de manera que, se pueda enfocar el cumplimiento de un criterio del modelo EFQM hacia el cumplimiento de un requisito de la norma ISO/IEC 27001.

- Se concluye acerca del análisis realizado, identificando las áreas de mejora en aras de cumplir los requisitos de la fase *Ejecución* del SGSI.

3.4.2.3. Resultados de la Fase 2.

Luego de realizar análisis de la evaluación de los criterios del marco de referencia propuesto para beneficio del cumplimiento de las cláusulas de la norma ISO 27001 se pudo determinar que DARCA no cuenta con un SGSI formalmente establecido. Al realizar la autoevaluación de cada uno de los criterios y sub-criterios del marco de referencia propuesto, se encontró que todos los criterios tienen una gran oportunidad de mejora. A continuación, se listan las oportunidades encontradas para cada criterio, con base resultados obtenidos en la autoevaluación.

- ✓ **Con respecto al Liderazgo**

Recordemos que el liderazgo es la base sobre la cual se fundamenta la implementación de un SGSI. La fase *Ejecución* de un SGSI requiere de grandes compromisos por parte de la alta dirección, y aún más teniendo en cuenta que esta es la primera iteración del ciclo PHVA. Gracias a la autoevaluación se pudieron determinar las siguientes oportunidades de mejora.

La alta dirección requiere:

- Participar e involucrarse en la creación y actualización de la política de seguridad de la información.
- Comprometerse con la política de seguridad de la información en aras de conseguir los recursos (físicos, tecnológicos, financieros) necesarios para poder establecerla.
- Dar prioridad a los asuntos relacionados con la seguridad de la información.
- Asegurar el funcionamiento de un SGSI en el procedimiento *Inscripciones y Admisiones*
- Comprometerse con la realización y ejecución del programa de implementación del SGSI, en aras de poder implementar controles de seguridad de la información.

- Revisar los resultados de las auditorías internas del SGSI, lo cual es la base para el mejoramiento del SGSI establecido en el procedimiento *Inscripciones y Admisiones*.

- Promover la realización de capacitaciones en seguridad de la información para el procedimiento *Inscripciones y Admisiones*.

- Conseguir los recursos necesarios para desarrollar los planes de mitigación de riesgos.

Finalmente se puede concluir que el desarrollo de la fase *Ejecución* de un SGSI requiere de una gran participación y acompañamiento por parte de la alta dirección de la Universidad del Cauca, es decir el rector.

- ✓ **Con respecto a la Estrategia (Programa de implementación del SGSI)**

El programa de implementación es el centro de la fase *Ejecución* de un SGSI. Por lo tanto, prestaremos especial atención a este elemento del marco de referencia propuesto. El programa de implementación de un SGSI toma como base los resultados obtenidos en la fase *Plan* del SGSI con el propósito de establecer unos objetivos de seguridad de la información y determinar un plan para lograr esos objetivos. Gracias a la autoevaluación se pudieron determinar las siguientes oportunidades de mejora.

El responsable del SGSI en el procedimiento *Inscripciones y Admisiones* requiere:

- Realizar un recuento de los resultados obtenidos en la fase *Plan* del SGSI para establecer la relación con la fase *Ejecución* del SGSI

- Establecer los objetivos de seguridad de la información que sean coherentes con la política de seguridad de la información.

- Comunicar los objetivos de la seguridad de la información dentro del alcance del SGSI.

- Establecer un plan para lograr los objetivos de seguridad de la información

- Especificar los recursos, responsables y la forma de evaluar los planes

- ✓ **Con respecto a las Personas**

El desarrollo de los planes anteriormente establecidos depende en gran medida de las personas. Por lo tanto, se requiere que las personas desarrollen unas determinadas competencias en seguridad de la información, y para lograr esto se emplean las capacitaciones. La formación de las personas tiene como propósito que las personas "tomen conciencia" de la importancia de la seguridad de la información y establezcan acciones que contribuyan con la fase *Ejecución* del SGSI. Gracias a la autoevaluación se pudieron determinar las siguientes oportunidades de mejora.

El procedimiento *Inscripciones y Admisiones* requiere:

- Establecer las competencias en seguridad de la información que deberían tener las personas que están relacionadas con el procedimiento *Inscripciones y Admisiones.*

- Evaluar las competencias en seguridad de la información que tienen las personas que se relacionan con el procedimiento *Inscripciones y Admisiones.*

- Solicitar y estimular el desarrollo de competencias en seguridad de la información por medio de formación y capacitación.

- Realizar una planificación para las capacitaciones en seguridad de la información, o solicitar que se incluya a DARCA en el programa de capacitaciones de la Universidad del Cauca. Especificar en la solicitud que las capacitaciones se realicen específicamente para el tema de la seguridad de la información.

- Propiciar y facilitar el desarrollo de capacitaciones en seguridad de la información al interior del procedimiento *Inscripciones y Admisiones* al menos una vez al año.

- Evaluar las competencias adquiridas por el personal que ha recibido algún tipo de capacitación y formación.

Todas las actividades realizadas en torno a la competencia y toma de conciencia benefician el buen funcionamiento o la implementación de un SGSI desde las prácticas realizadas por los empleados.

- ✓ **Con respecto a los Alianzas y Recursos**

Las dependencias de la Universidad del Cauca han desarrollado alianzas entre sí, y se engranan para cumplir la misión, visión y objetivos de la Universidad. De la misma manera se deben desarrollar las alianzas correspondientes entre el procedimiento *Inscripciones y Admisiones* y otras dependencias de la Universidad del Cauca para cumplir los objetivos de seguridad establecidos. Gracias a la autoevaluación se pudieron identificar las siguientes oportunidades de mejora.

El procedimiento *Inscripciones y Admisiones* requiere:

- Solicitar y/o distribuir los recursos financieros necesarios implementar un SGSI.
- Optimizar los recursos físicos y materiales existentes en el procedimiento *Inscripciones y Admisiones*.
- Buscar e implicar aquellos grupos de interés en el desarrollo de los planes del programa de implementación del SGSI
- Buscar e implicar aquellos grupos de interés relacionados con tecnologías existentes y novedosas en el desarrollo de los planes del programa de implementación del SGSI
- Establecer y mantener comunicaciones con áreas externas a DARCA y proveedores, para el fortalecimiento del SGSI en el procedimiento *Inscripciones y Admisiones.*
- Mantener y mejorar las alianzas establecidas hasta el momento con entidades externas a DARCA.

- ✓ **Con respecto a los procesos, productos y servicios (Procedimientos del SGSI)**

Para llevar a cabo los procesos de un SGSI es necesario que existan un conjunto de *procedimientos documentados* que especifiquen el paso a paso a seguir. Los procedimientos documentados dicen cómo llevar a cabo los procesos para establecer implementar, mantener y mejorar el SGSI. Gracias a la autoevaluación se pudieron identificar las siguientes oportunidades de mejora.

El procedimiento *Inscripciones y Admisiones* de DARCA requiere elaborar y establecer formalmente los siguientes procedimientos para el SGSI:

- Procedimiento de control de registros.
- Procedimiento operativo del SGSI
- Procedimiento de auditoria interna del SGSI
- Procedimiento de acciones preventivas
- Procedimiento de acciones correctivas
- Procedimiento de comunicaciones internas y externa

El procedimiento *Inscripciones y Admisiones* requiere que:

- Se realicen los procesos correspondientes al SGSI con base en los pasos establecidos en los *procedimientos documentados*
- Al realizar los procesos se elaboren reportes, registros y documentos
- Se comuniquen a los grupos de interés, los procesos a llevar a cabo.
- Se realice una planificación para cada proceso a llevar a cabo

✓ **Con respecto a los Resultados del SGSI**

Los resultados de la fase *Ejecución* del SGSI se evidencian principalmente por el uso de métricas y de auditorías internas. En este trabajo de grado solo abordamos lo correspondiente a métricas, ya que la parte de auditoria corresponde a la fase "Verificar" según el ciclo Deming. En este orden de ideas solo se evalúan las oportunidades de mejora correspondiente a métricas. Gracias a la autoevaluación se pudieron identificar las siguientes oportunidades de mejora.

Se requiere que el jefe de DARCA:

- Revise los resultados del SGSI a intervalos planificados.
- Solicite una auditoria interna del SGSI dentro del alcance del procedimiento *Inscripciones y Admisiones* (Para trabajos futuros)
- Verifique el desarrollo de mediciones para los controles de seguridad de la información

3.4.3. Fase 3. Elaboración y despliegue de Planes de acción para el cumplimiento de las cláusulas de la Fase Ejecución del SGSI.

3.4.3.1. Descripción de la Fase 3.

La tercera fase consiste en la elaboración de planes de acción con base en los resultados de evaluación de la segunda fase. Se deben desarrollar planes de acción teniendo en cuenta los aspectos más relevantes para el alcance del procedimiento *Inscripciones y Admisiones*. A cada plan se le establece una prioridad, que determina el orden en el cual se van a desplegar.

La Tabla XV presenta el objetivo, actividades, indicador y producto de trabajo correspondiente a la tercera fase.

TABLA XV. Descripción de la tercera fase del marco de referencia propuesto

Elaboración y despliegue de los planes de acción	
Objetivos: Elaborar planes de acción, identificando la prioridad de cada uno de ellos. Desplegar los planes de acción obedeciendo el orden de prioridad establecido.	
Actividades	**Indicador**
– Priorizar las oportunidades – Asignar un responsable al desarrollo de los planes – Elaborar los planes de acción – Poner en marcha las tareas presentes en los planes.	– Elaboración y desarrollo de los planes de acción
Producto de trabajo: Documento del plan de acción. Documentos y registros de acciones realizadas	

3.4.3.2. Desarrollo y Resultados de la Fase 3.

- ✓ **Elaboración de los planes de acción**

Los planes de acción se realizaron con base en las oportunidades identificadas en la segunda fase (de autoevaluación). Las oportunidades de mejora encontradas en la autoevaluación del procedimiento *Inscripciones y Admisiones* son muchas, y por cuestiones de tiempo, pertinencia y recursos no podremos abordarlas todas. Por lo tanto, para realizar los planes de acción se deben elegir algunas.

Es importante reconocer que todas las oportunidades de mejora identificadas anteriormente, son de relevancia para la implementación del SGSI, y contribuyen

con la excelencia de una u otra manera. Sin embargo, se eligen aquellas oportunidades están en concordancia con los requisitos de la norma ISO/IEC 27001 para la fase *Ejecución* de un SGSI. En este orden se ideas se eligen, los aspectos que se muestran en la Tabla XVI.

TABLA XVI. Oportunidades de mejora seleccionadas

Requisito de ISO/IEC 27001	**Oportunidad**
Liderazgo	– Comprometerse con la política de seguridad de la información. – Comprometerse con la realización e implementación de uno o más controles de seguridad de la información.
Programa de implementación	– Establecer los objetivos de seguridad de la información que sean coherentes con la política de seguridad de la información. – Comunicar los objetivos de la seguridad de la información dentro del alcance del SGSI. – Establecer un plan para lograr los objetivos de seguridad de la información – Especificar los recursos, responsables y la forma de evaluar los planes
Competencia y toma de conciencia	– Realizar una planificación para las capacitaciones en seguridad de la información, o solicitar que se incluya a DARCA en el programa de capacitaciones de la Universidad del Cauca. Especificar en la solicitud que las capacitaciones se realicen específicamente para el tema de la seguridad de la información. – Propiciar y facilitar el desarrollo de capacitaciones en seguridad de la información al interior del procedimiento *Inscripciones y Admisiones* al menos una vez al año.
Recursos	– Optimizar los recursos físicos y materiales existentes en el procedimiento *Inscripciones y Admisiones*.
Procedimientos del SGSI	Elaborar los siguientes procedimientos: – Procedimiento de control de registros. – Procedimiento operativo del SGSI – Procedimiento de auditoria interna del SGSI – Procedimiento de acciones preventivas – Procedimiento de acciones correctivas – Procedimiento de comunicaciones internas y externa
Resultados del SGSI	– Verifique el desarrollo de mediciones para los controles de seguridad de la información

Para realizar los planes de acción se tuvieron en cuenta los controles de seguridad de la información y los planes de mitigación de riesgos (descritos en la sección 3.2 de este documento), además de las oportunidades de la tabla anterior. En definitiva, se establecieron dos planes de acción, uno corresponde al control “políticas”, y otro correspondiente al control “Concienciación”. Estos dos planes elaborados se pueden ver en el ***Anexo F***. Los planes de acción realizados se presentaron al jefe DARCA y fueron aprobados.

- ✓ **Despliegue de los planes de acción**

Para efectos de este trabajo de grado los responsables de ejecutar los planes de acción son los estudiantes. Sin embargo, es necesario establecer responsabilidades al interior de la Universidad del Cauca para realizar y desarrollar nuevos planes de acción.

A continuación, se procedió a llevar a cabo los planes de acción. Para cada uno de los planes de acción o planes de proyecto se llevaron a cabo las siguientes fases:

- **Evaluación del estado actual**: Se determina es estado de cada uno de los controles para el procedimiento *Inscripciones y Admisiones.* En consecuencia, se pudieron establecer los estados que se muestran en la Tabla XVII.

TABLA XVII. Estado inicial de los controles a implementar

Control	Estado Inicial
A.5.1.1 Políticas de seguridad de la información	Ausente
A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Ausente

- **Estructuración de los procedimientos:** En esta sección se elaboró el procedimiento que se debe seguir para realizar capacitaciones en seguridad de la información y el procedimiento para la evaluación, actualización y eliminación de políticas de seguridad de la información. Estos procedimientos son la guía para realizar los planes de proyecto, y se muestran en el ***Anexo G***.

- **Entrenamiento:** Antes de realizar las capacitaciones y dar a conocer la política de seguridad en la información, fue necesario realizar un entrenamiento en los temas de interés. En este caso se procedió a revisar la documentación y videos de los siguientes temas:

- Política general de seguridad para el procedimiento *Inscripciones y Admisiones*
- Acceso por parte de terceros
- Protección contra virus
- Copias de seguridad o respaldo
- Seguridad de contraseñas
- Administración de acceso a funcionarios

- **Puesta en marcha:** En esta parte se procede a emplear la Guía número 2 del MSPI para documentar formalmente la política de seguridad de la información. La política fue revisada y documentada según se muestra en el **Anexo I.**

- **Reportes:** La política fue comunicada a los funcionarios de DARCA, y para ello se realizaron varias reuniones, cuyas evidencias se muestran en el **anexo J**.

  Las capacitaciones se realizaron en las instalaciones de DARCA y los registros de su realización también se muestran en el **anexo J**.

3.4.4. Fase 4. Validación y realimentación de los resultados

3.4.4.1. Descripción de la Fase 4.

La cuarta fase consiste en determinar el cumplimiento o no de los planes de acción por medio de una validación de las actividades y registros. Luego se realiza un seguimiento a los resultados de las cuatro fases, con el propósito de identificar aspectos clave para la mejora continua. La Tabla XVIII presenta el objetivo, actividades, indicadores y producto correspondiente a la tercera fase.

La cuarta fase del marco de referencia propuesto consiste en revisar los resultados obtenidos con la ejecución de los planes de acción o planes de proyecto. Para ello se volvió a evaluar el estado de los controles, y como resultado se obtuvo que las los dos controles se encuentran en un estado “Insuficiente”. Estos dos controles se llevaron a cabo con muchas dificultades, por lo cual existen muchos aspectos por mejorar.

El jefe de DARCA apoyó continuamente los planes de acción, sin embargo, la disponibilidad de tiempo fue muy limitada. El jefe de DARCA estuvo muy pendiente de la ejecución de los planes de acción, y concluyó que las políticas deben ser mejoradas y aplicadas gradualmente.

TABLA XVIII. Descripción de la cuarta fase del marco de referencia propuesto

<table>
<tr><th colspan="2">Validación y realimentación</th></tr>
<tr><td colspan="2">Objetivo: Revisar los resultados del proceso realizado en las fases operativas anteriores e identificar aspectos clave para el establecimiento de proyectos de mejora continua</td></tr>
<tr><th>Actividades</th><th>Indicador</th></tr>
<tr><td>– El jefe DARCA debe confrontar el cumplimiento de los planes de acción.
– El jefe DARCA realiza seguimiento de todo el proceso operativo realizado hasta el momento en aras de identificar fortalezas, debilidades y oportunidades de mejora
– Plantear posibles proyectos de mejoramiento</td><td>– Evaluación y seguimiento de los resultados obtenidos y planteamiento de proyectos de mejoramiento</td></tr>
<tr><td colspan="2">– Producto de trabajo: Informe de los resultados de los planes de acción
Informe de proyectos de mejora</td></tr>
</table>

El jefe de DARCA llegó a la conclusión de que las capacitaciones en seguridad de la información deben realizarse de manera continua, y que se dicten con personal especializado. Con lo cual se requiere el apoyo de áreas como gestión de calidad y talento humano de la Universidad del Cauca. Finalmente, el jefe de DARCA expresa su preocupación por continuar con el mejoramiento de los dos controles implementados.

3.4.4.2. Desarrollo y Resultados de la Fase 4

La cuarta fase del marco de referencia propuesto consiste en revisar los resultados obtenidos con la ejecución de los planes de acción o planes de proyecto. Para ello se volvió a evaluar el estado de los controles, y como resultado se obtuvo que las los dos controles se encuentran en un estado “Insuficiente”. Estos dos controles se llevaron a cabo con muchas dificultades, por lo cual existen muchos aspectos por mejorar.

El jefe de DARCA apoyó continuamente los planes de acción, sin embargo, la disponibilidad de tiempo fue muy limitada. El jefe DARCA estuvo muy pendiente de la ejecución de los planes de acción, y concluyó que las políticas deben ser mejoradas y aplicadas gradualmente. El ***Anexo H*** muestra la política formalmente establecida para el procedimiento *Inscripciones y Admisiones.* El ***Anexo I*** muestra los registros de las capacitaciones realizadas en este procedimiento.

El jefe DARCA llegó a la conclusión de que las capacitaciones en seguridad de la información deben realizarse de manera continua, y que se dicten con personal especializado. Con lo cual se requiere el apoyo de áreas como gestión de calidad y talento humano de la Universidad del Cauca. Finalmente, el jefe DARCA expresa su preocupación por continuar con el mejoramiento de los dos controles implementados.

- ✓ **Procedimientos documentados propuestos**

  Como parte final de este trabajo de grado se realizaron los procedimientos que se muestran en el ***Anexo J***. Estos procedimientos se realizaron para dejar planteados los artefactos operacionales del SGSI, y adicionalmente se deja planteado el procedimiento de auditoria interna para que se utilice en la fase *Verificación* del SGSI. Los procedimientos propuestos son:

  - Procedimiento de Control de Registros
  - Procedimiento operativo del SGSI
  - Procedimiento de auditoria interna del SGSI.
  - Procedimiento de acción preventiva
  - Procedimiento de acción correctiva
  - Procedimiento de las comunicaciones

4. CAPITULO V. CONCLUSIONES, APORTES Y TRABAJOS FUTUROS

4.1. CONCLUSIONES

4.1.1. Conclusiones del proceso de armonización

El proceso de armonización fue significativamente facilitado empleando HProcess, estableciendo a su vez múltiples beneficios como la reducción de la subjetividad al momento de comparar dos modelos y/o estándares múltiples, a la vez que se establecen roles claros y productos de trabajo que permiten evidenciar el cumplimiento de las actividades.

El proceso de armonización definido en HProcess establece una guía de uso general que reduce el esfuerzo de comprensión de los modelos y/o estándares a armonizar, estableciendo una estructura común a través del método de homogenización, lo cual permite identificar las relaciones y diferencias de los marcos a armonizar.

El proceso de armonización definido en HProcess no define una estructura única, sino que se puede ajustar a las necesidades de armonización. En este sentido, las necesidades de armonización de la organización determinan el establecimiento de la estrategia de armonización.

4.1.2. Conclusiones del marco propuesto

El enfoque del marco de referencia propuesto beneficia el mejoramiento de las practicas relacionadas con la gestión del sistema de seguridad de la información exigidas por la norma ISO/IEC 27001:2013, lo cual se debe a que las practicas del modelo EFQM complementan las prácticas de la norma.

El marco propuesto aprovecha el concepto de autoevaluación del modelo EFQM y lo enfocado hacia la verificación de los requisitos de la fase *Ejecución* del SGSI con respecto al procedimiento *Inscripciones y Admisiones.*

La direccionalidad del marco de referencia propuesto toma como base la norma ISO 27001, de manera que las practicas del modelo EFQM se emplean para beneficiar el cumplimiento de los requisitos de la norma en miras hacia una futura certificación del procedimiento *Inscripciones y Admisiones.*

El marco de referencia propuesto permitió mejorar las practicas encaminadas al cumplimiento de las cláusulas de la norma ISO 27001 realizadas el procedimiento *Inscripciones y Admisiones,* beneficiando así el mejoramiento de los procesos.

4.1.3. Conclusiones de la implementación de la fase *Ejecución* del SGSI

La ausencia de conocimientos por parte de los investigadores en los temas de SGSI, norma ISO/IEC 27001, modelo EFQM y marcos de referencia empleados en la implementación de un SGSI; dificultaron el normal desarrollo de las actividades planteadas en el anteproyecto, por lo cual se concluye que la implementación de un SGSI puede llegar a ser algo muy complejo cuando no se cuenta con personal experto.

La ausencia de conocimiento por parte de los funcionarios de DARCA en la terminología de seguridad de la información y la norma ISO/IEC 27001 dificultaron la comprensión de este proyecto, por lo que se comenzó socializando la política del SGSI de la Universidad del Cauca. Luego, la socialización de la fase *Planear* del SGSI en el procedimiento *Inscripciones y Admisiones*, y finalmente, la socialización de los programas a desarrollar en la fase *Ejecución.* Con lo cual se concluye que el

éxito en la implementación de un SGSI, depende en gran medida del desarrollo de las competencias en seguridad de la información de los funcionarios de DARCA.

Antes de comenzar a abordar este proyecto de investigación, fue necesario tener un pleno conocimiento de la fase *Planear* del SGSI y del procedimiento *Inscripciones y Admisiones*. Además, fue necesario realizar actividades, procedimiento y registros que correspondían a la fase *Planear* del SGSI, debido a que no se encontraron las respectivas evidencias. Con lo cual se concluye que el éxito de la implantación del SGSI depende en gran medida del buen desarrollo de la fase *Planear*. Adicionalmente se corrobora que la implantación de un SGSI necesita gran cantidad de recursos, como tiempo y acompañamiento de personal experto.

Se realizó un programa de implementación de SGSI que incluyó un programa de implementación para cada control de seguridad de la información. Luego, se dio cumplimiento a las actividades, y esto conllevó finalmente al cumplimiento de los objetivos trazados en seguridad de la información. Con lo cual se concluye que para cada control de seguridad es preciso diseñar y ejecutar de un programa de implementación.

El jefe de DARCA aporto con su disposición y su tiempo, en ocasiones por fuera del horario laboral, para el desarrollo de las actividades correspondientes a la fase *Ejecución* del SGSI. Adicionalmente los funcionarios de DARCA contribuyeron con el desarrollo de las actividades de capacitación de políticas y toma de conciencia. Con lo cual se concluye que la implementación de la fase *Ejecución* del SGSI se logró gracias al apoyo continuo del jefe de DARCA y de todos los funcionarios. Sin su apoyo esto no habría sido posible.

El Modelo EFQM aportó a la implementación de la fase *Ejecución* del SGSI, basándose en la aplicación de un ciclo de mejora continua. Este ciclo del modelo EFQM se aplicó a la implantación de los controles de seguridad de la información seleccionados. Con esto se concluye que el Modelo EFQM se aplica para el mejoramiento de los controles implementados.

La implantación del SGSI en el procedimiento *Inscripciones y Admisiones* es un proyecto de gran envergadura que no termina con este proyecto de investigación, ya que la seguridad de la información en DARCA y en la Universidad del Cauca tiene mucho por recorrer.

Se logró capacitar a los funcionarios de DARCA con respecto al cumplimiento de las políticas de seguridad de la información, brindando recomendaciones para el mejoramiento de sus competencias en el desarrollo de su trabajo.

DARCA no cuenta con las competencias necesarias para hacerse responsable de la operación y supervisión de un SGSI en el procedimiento *Inscripciones y Admisiones*, por lo cual se necesita que la Universidad del Cauca designe un responsable del SGSI institucional.

DARCA requiere la aplicación de controles que demandan acompañamiento y apoyo de áreas como Talento Humano, División de las TIC, Gestión de la Calidad y Vicerrectoría Académica. Por ejemplo, la aplicación del procedimiento de auditoria interna en DARCA requiere del acompañamiento del área de Control Interno de la Universidad del Cauca.

La implementación de un SGSI en el procedimiento *Inscripciones y Admisiones* contribuyó con el mejoramiento de se seguridad de la información de DARCA, derivada de un mejor comportamiento en cuanto a la protección de los activos de información. Además, este proyecto de investigación aporta significativamente a la competitividad de la Universidad del Cauca, incursionando en el procedimiento *Inscripciones y Admisiones* con respecto al cumplimiento de la norma NTC-ISO/IEC 27001.

4.2. APORTES

Los aportes de este trabajo de grado están divididos en dos componentes. El primero de ellos es un componente de *Innovación,* que está constituido por la adaptación de un marco de referencia en base a la norma ISO/IEC 27001:2013 y el modelo EFQM. El segundo aporte está enfocado en el desarrollo, de manera que se emplea el modelo propuesto para realizar la fase *Ejecución* del SGSI en el procedimiento *Inscripciones y Admisiones*, perteneciente a DARCA de la Universidad del Cauca.

4.3. RECOMENDACIONES

Se recomienda implementar nuevos controles de seguridad de la información que deben ser seleccionados de la Declaración de Aplicabilidad – SOA (Ver sección 3 del Anexo A). En este sentido, se recomienda Implementar controles que se encuentren en el Dominio “Control de Acceso” del anexo A de la norma NTC-ISO/IEC 27001, lo cual beneficia a DARCA debido a sus características y necesidades. Además, se recomienda Implementar controles que se encuentren en el Dominio “Seguridad Física y del Entorno”.

Se recomienda emplear el marco de referencia propuesto para optimizar los dos controles implementados con el propósito de obtener resultados que se puedan sostener y mejorar a lo largo del tiempo.

De ser posible, se recomienda contar con la ayuda de un experto entrenado que tenga el aval del rector de la Universidad del Cauca para auditar el SGSI de DARCA, y al finalizar pueda dar recomendaciones específicas que contribuyan al cumplimiento de la norma NTC-ISO/IEC 27001. En su defecto, se recomienda capacitar a una persona de la Universidad del Cauca como auditor interno en la norma NTC-ISO/IEC 27001, para auditar a DARCA y a otros departamentos.

Se recomienda solicitar al área de "Gestión de la Calidad" incluir la seguridad de la información en su programa de capacitaciones, y tramitar las acciones necesarias para que los funcionarios de DARCA reciban dos capacitaciones por año por parte de personal especializado.

Se recomienda que el jefe de DARCA solicite a quien corresponda, el desarrollo de capacitaciones relacionadas con amenazas naturales como sismos o terremotos con el fin de desarrollar planes de contingencia para el desarrollo del procedimiento *Inscripciones y Admisiones* de DARCA.

Se recomienda que la Universidad del Cauca designe un área o departamento responsable de la seguridad de la información, diferente a DARCA, que cuente con el personal competente y con la autoridad suficiente para impulsar actividades que tengan un mayor impacto en la seguridad de la información de la institución.

Teniendo en cuenta la complejidad de la Universidad del Cauca se recomienda conformar un equipo interdisciplinario de seguridad de la información, con la participación de por lo menos una persona de cada departamento, con el fin de que el macro proyecto de seguridad de la información de la Universidad del Cauca [15] pueda conocerse en toda la institución, y se comience a realizar acciones efectivas que contribuyan al cumplimiento de los requisitos especificados en la norma NTC-ISO/IEC 27001, en miras hacia una futura certificación institucional de la norma.

4.4. TRABAJOS FUTUROS

Para apoyar este proyecto y otros proyectos relacionados con SGSI se recomienda desarrollar proyectos para la realización de una aplicación software genérica que sirva de guía en la implementación de un SGSI conforme a la norma ISO/IEC 27001 en cualquier departamento o institución.

Realizar la fase *Verificar* del SGSI según el ciclo Deming con el propósito de revisar y evaluar regularmente el SGSI implementado. Para ello es necesario tomar como base los resultados obtenidos en este trabajo de investigación.

Aplicar el marco de referencia y los procedimientos propuestos en este proyecto para desarrollar la fase *Ejecución* de un SGSI en los sub procedimientos o divisiones de la Universidad del Cauca que hayan desarrollado la fase *Plan* de un SGSI.

REFERENCIAS

[1] D. Cantón, “Titulares de ciberseguridad del 2015,” *Incibe.es*, 2016. [Online]. Available: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Titulares_de_ciberseguridad_del_2015. [Accessed: 01-Mar-2016].

[2] “Ciberataques, Ciberamenazas, Privacidad y Delitos Informáticos,” *Gitsinformatica.com*, 2015. [Online]. Available: http://www.gitsinformatica.com/ciberataques.html. [Accessed: 01-Mar-2016].

[3] Consejo Nacional de Política Económica y Social CONPES, “Politica Nacional de Seguridad Digital,” *Departamento Nacional de Planeación*. Bogota, D.C., 2016.

[4] Comisión de Regulación de Comunicaciones CRC, “Identificación de las posibles acciones regulatorias a implementar en materia de Ciberseguridad Documento de análisis y consulta,” Colombia, 2015.

[5] Corporación Colombia Digital, “Organizaciones colombianas no están preparadas ante riesgos informáticos,” *colombiadigital.net*, 2015. [Online]. Available: http://colombiadigital.net/actualidad/noticias/item/8168-organizaciones-colombianas-no-estan-preparadas-ante-riesgos-informaticos.html. [Accessed: 01-Mar-2016].

[6] Telefónica, “4 de cada 10 empresas en Colombia no están preparadas para un ciberataque,” Bogotá. D.C., 2016.

[7] The International Organization for Standardization and The International Electrotechnical Commission, *Information technology - Security techniques - Information security management systems - Requirements*. ISO/IEC 27001, 2013.

[8] *Information technology - Security techniques - Information securiry managenent system - Overview and vocabulary*. ISO/IEC 27000, 2016.

[9] The International Organization for Standardization and The International Electrotechnical Commission, *Information technology - Security techniques - Code of practice for information security controls*. ISO/IEC 27002, 2013.

[10] The International Organization for Standardization and The International Electrotechnical Commission, *Information technology - Security techniques - Information security management system - Implementation guidance*. ISO/IEC 27003, 2010.

[11] The International Organization for Standardization and The International Electrotechnical Commission, *Information technology - Security techniques - measurement*. ISO/IEC 27004, 2009.

[12] The International Organization for Standardization and The International Electrotechnical Commission, *Information technology - Security - Information security risk management*. ISO/IEC 27005, 2011.

[13] J. Garcia, *PDCA Ciclo de Deming*. 2011.

[14] J. P. Martinez Pulido and D. F. Espinosa Tafur, “Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC 27005:2011, proponiendo una adaptación de la metodología OCTAVE-S. Caso de estudio: Proceso Inscripciones y Admisiones en DARCA,” 2015.

[15] División de Tecnologías de la información y las Comunicaciones, “Sistema de Gestión de la Seguridad de la Informacion de la Universidad del Cauca,” Popayán, 2015.

[16] Y. Wadsworth, “What is participatory Action Research?,” *Action Research International (Paper 2)*, 1998. [Online]. Available: http://www.aral.com.au/ari/pywadsworth98. [Accessed: 01-Aug-2013].

[17] F. J. Pino, M. Piattini, and G. Horta Travassos, “Gestión y desarrollo de proyectos de investigación distribuidos en ingeniería del software por medio de investigación-acción,” *Rev. Fac. Ing.*, no. 68, pp. 61–74, 2013.

[18] W. French and C. Bell, *No Title*, 6th ed. London, England., 1999.

[19] V. M. Niño Rojas, “Metodologia de la Investigacion: Diseño y Ejecucion,” Bogotá D.C.: edicionesdelau.com, 2011, pp. 85–108.

[20] “Capítulo 2. modelos y estándares de calidad de software,” pp. 10–18, 1998.

[21] F. Scalone, “Estudio compatativo de los Modelos y Estándaresde calidad del Software,” Universidad Tecnológica Nacional, 2006.

[22] C. J. Pardo Calvache, F. O. García Rubio, F. J. Pino Correa, and M. Piattini Velthuis, “A Framework to Support the Harmonization between Multiple Models and Standards,” University of Castilla - La Mancha, 2012.

[23] C. de Nieves Nieto and L. Ros McDonnell, “Comparación entre los Modelos de Gestión de Calidad Total: EFQM, Gerencial de Deming, Iberoamericano para la Excelencia y Malcom Baldrige. Situación frente a la ISO 9000,” *X Congr. Ing. Organ.*, 2006.

[24] M. Araújo, “ISO 9001: 2015 es incompatible con la estandarización de procesos y la burocracia,” *Qualitu Way*, 2017. [Online]. Available: https://qualityway.wordpress.com/2017/02/12/a-iso-90012015-e-incompativel-com-padronizacao-de-processos-e-burocracia-por-manoel-m-de-souza-araujo/. [Accessed: 01-Aug-2017].

[25] A. Crrión García, “EL MODELO EFQM. Más allá de ISO 9000.,” pp. 105–110, 2006.

[26] P. Corredor and S. Goñi, “Tipos de premios a la calidad y efectos sobre la rentabilidad de la empresa,” *Rev. Española Financ. y Contab.*, vol. 39, no. 148, pp. 637–654, 2010.

[27] E. Suárez, J. Roldan, and A. Mora, “Análisis estructural del modelo EFQM de excelencia: el papel mediador de la gestión por procesos y la planificación estratégica,” Universidad de Sevilla, 2017.

[28] E. Suárez, J. L. Roldán, and A. Calvo-Mora, “Análisis estructural del modelo EFQM: una evaluación del papel de mediación del proceso de administración,” *J. Bus. Econ. Manag.*, vol. 15, no. 5, pp. 862–885, 2014.

[29] Microdeco, “Nos dieron el Premio Europeo a la Responsabilidad Social,” 2011.

[30] A. Bayo, J. Díaz, S. Escamilla, and R. Selvam, “The impact of ISO 9000 and EFQM on the use of flexible work practices,” *Int. J. Prod. Econ.*, vol. 130, pp. 33–42, 2011.

[31] Nextel S.A., “ISO 20000, camino a la excelencia,” 2011.

[32] Universidad de Navarra, “Implanación del modelo EFQM en Navarra. Incidencia en la competitividad empresarial y generación de empleo.,” 2014.

[33] F. Navarro, “El modelo EFQM. Criterios de excelencia empresarial.,” 2016. [Online]. Available: https://revistadigital.inesem.es/gestion-integrada/el-modelo-efqm-criterios-de-excelencia-empresarial/. [Accessed: 01-Aug-2017].

[34] J. J. Sánchez Peña, “Alineando ITIL, COBIT Y EFQM.,” 2015.

[35] A. Cabrero and F. Soler, “ITIL, ISO 9001 y EFQM: la convivencia es posible. Caso Práctico,” 2014.

[36] L. C. Aliaga Flores, “Diseño de un Sistema de Gestión de Seguridad de la Información para un instituto educativo,” 2013.

[37] S. Zhang and H. Le Fever, “An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model,” *J. Econ. Bus. Manag.*, vol. 1, pp. 391–395, 2013.

[38] M. Gehrmann, “Combining ITIL, COBIT and ISO / IEC 27002 for structuring comprehensive information technology for management in organizations,” *Navus - Rev. Gest. e Tecnol.*, vol. 2, pp. 66–77, 2012.

[39] S. Tyali, “An Integrated Management System for Quality and Information Security in Healthcare,” 2012.

[40] Q. Liu, Q. Du, W. Shi, and J. Zhu, “Modeling of risk treatment measurement model under four clusters standards (ISO 9001, 14001, 27001, OHSAS 18001),” *Procedia Eng.*, vol. 37, pp. 354–358, 2012.

[41] V. Montaño Orrego, “La gestión en la seguridad de la información según Cobit, Itil e Iso 27000,” *Rev. Pensam. Am.*, vol. 2, pp. 21–23, 2013.

[42] F. O. F. Business, “Propuesta de procesamiento de documentación para la certificación de una empresa que preste servicios integrados de seguridad informática.,” 2016.

[43] B. Barafort, A. L. Mesquida, and A. Mas, “Integrating risk management in IT settings from ISO standards and management systems perspectives,” *Comput. Stand. Interfaces*, vol. 54, pp. 176–185, 2017.

[44] M. F. Rebelo, G. Santos, and R. Silva, “Integration of management systems: towards a sustained success and development of organizations,” *J. Clean. Prod.*, vol. 127, pp. 96–111, 2016.

[45] A. Fernández and L. J. Ramírez, “Alineación de la norma iso 9001:2008 con la norma iso 28000:2007 para una empresa de seguridad privada,” 2015.

[46] R. Ferro Escobar, G. M. Tarazona Bermudez, and G. A. Alzate Acuña, “Implementación de procedimientos de gobernabilidad TI en la red de investigación de tecnología avanzada basado en ITIL, COBIT y la ISO 20000-27000,” *E ISSN 2248 Edición Espec.*, vol. 6, pp. 37–44, 2015.

[47] D. R. Plata Arango, “¿De ISO 20000 e ISO 27001 la evocución hacia un modelo de gobernanza empresarial de TI?,” *TICAL2014*, 2014.

[48] D. R. Plata Arango, “Estrategias para la implementación de ISO 20000 E ISO 27001 en una universidad pública colombiana,” *TICAL2013*, 2013.

[49] O. L. García Jiménez and D. C. Acosta Rodríguez, “ISO 9001-2008 y EFQM: Un Estudio Comparativo para su Implementación en la Educación,” Pontificia Universidad JAVERIANA, 2010.

[50] L. J. Mora Potosi and F. A. Chavarro Florez, “Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC 27005:2011, adaptando la metodología NIST SP 800-30. Caso de estudio: Procedimiento Gestión de Servicios y Servidores de Internet en la División TIC de la Universidad del Ca,” Universidad del Cauca, Popayán, 2016.

[51] M. A. Galindez Muñoz and J. H. Reyes Cerón, “Gestión del riesgo del SI con base en la norma ISO/IEC 27005:2011 adaptando la metodología MAGERIT V3 para el caso de estudio propuesto,” Universidad del Cauca, Popayán, 2016.

[52] Z. D. Kelemen, J. Trienekens, R. Küsters, and K. Balla, “A process based unification of process-oriented software quality approaches,” *Proc. - 2009 4th IEEE Int. Conf. Glob. Softw. Eng. ICGSE 2009*, no. January 2014, pp. 285–288, 2009.

[53] Software Engineering Institute - SEI, “PrIME,” 2017. [Online]. Available: http://www.sei.cmu.edu/process/research/prime-details.cfm. [Accessed: 20-Feb-2007].

[54] A. Ferchichi, J. P. Bourey, M. Bigand, and H. Lefebvre, “Implementing integration of quality standards Capability Maturity Model Integration and ISO 9001:2000 for software engineering,” *Int. J. Prod. Lifecycle Manag.*, vol. 2, no. 4, pp. 356–385, 2007.

[55] Software Engineering Institute Carnegie Mellon University, “IDEAL: A User’s Guide for Software Process Improvement,” *CMU/SEI-96-HB-001*, 1996. [Online]. Available: http://www.sei.cmu.edu/publications/documents/96. [Accessed: 01-Feb-2017].

[56] L. Scott, R. Jeffery, L. Carvalho, J. D’Ambra, and P. Rutherford, “Practical Software Process Improvement - the IMPACT project,” *Proc. 2001 Aust. Softw. Eng. Conf.*, pp. 182–189, 2001.

[57] C. J. Pardo-Calvache, F. O. García-Rubio, M. G. Piattini-Velthuis, F. J. Pino-Correa, and M. T. Baldassarre, “A 360-degree process improvement approach based on multiple models,” *Rev. Fac. Ing. Univ. Antioquia*, vol. 2015, no. 77, pp. 95–104, 2015.

[58] C. Pardo, F. J. Pino, F. García, and M. Piattini, “Homogenization of models to support multi-model processes in improvement environments,” *ICSOFT 2009 - 4th Int. Conf. Softw. Data Technol. Proc.*, vol. 1, pp. 151–156, 2009.

[59] C. Pardo, F. J. Pino, F. García, M. Piattini, and M. T. Baldassarre, “Trends in Harmonization of Multiple Reference Models,” *L.A. Maciaszek, P. Loucopoulos (Eds.), ENASE 2010, CCIS, Springer-Verlag, Berli Heidelb.*, pp. 61–73, 2011.

[60] C. Pardo, F. J. Pino, F. García, M. Piattini, and M. T. Baldassarre, “An ontology for the harmonization of multiple standards and models,” *Comput. Stand. Interfaces*, vol. 34, no. 1, pp. 48–59, 2012.

[61] C. Pardo, F. J. Pino, F. García, M. Piattini, and M. T. Baldassarre, “A Process for Driving the Harmonization of Models,” pp. 51–54, 2010.

[62] C. Pardo, F. García, F. J. Pino, M. Piattini, and M. T. Baldassarre, “Método de integración para soportar la armonización de múltiples modelos y estándares,” 2011.

[63] C. Pardo, F. J. Pino, F. Garcia, M. T. Baldassarre, and M. Piattini, “From chaos to the systematic harmonization of multiple reference models: A harmonization framework applied in two case studies,” *J. Syst. Softw.*, vol. 86, no. 1, pp. 125–143, 2013.

[64] C. Pardo, F. J. Pino, and F. Garcia, “Towards an Integrated Management System (IMS), harmonizing the ISO/IEC 27001 and ISO/IEC 20000-2 standards,” *Int. J. Softw. Eng. its Appl.*, vol. 10, no. 9, pp. 217–230, 2016.

[65] M. Cuellar, C. Pardo, L. Herrera, and M. Correa, “Armonización de múltiples modelos para el gobierno de TI y el desarrollo de software,” *Vent. Informática*, no. 30, pp. 43–53, 2014.

[66] Universidad del Cauca, “Manual de Procesos y Procedimientos.” p. 15, 2011.

[67] Universidad del Cauca, “Mapa de Procesos - Universidad del Cauca.” 2014.

[68] Universidad del Cauca, “Despliegue de procesos Institucionales.” 2014.

[69] G. S. Carlos Alberto, “Diseño de un Sistema de Información para una Entidad Financiera de Segundo Piso,” Institución Universitaria Politécnico Grancolombiano, 2015.

[70] G. Pallas, “Metodología de Implantación de un SGSI en un grupo empresarial jerárquico,” Universidad de la Republica, 2009.

[71] R. D. Carvajal Herrera, “Seguridad Informática y de la Información,” 2013.

[72] R. Baldecchi, “Implementación efectiva de un SGSI ISO 27001,” *2014*, p. 3, 2014.

[73] The International Organization for Standardization, “Iso/Iec 27000:2016,” *ISO.org [Online]*, vol. 2016, p. 38, 2016.

[74] “Ciclo PHVA (Planificar - Hacer - Verificar - Actuar).”

[75] A. Gallo Oñate, “Diagnóstico de cumplimiento del modelo gestionado por el sistema de administración de la seguridad de la información de gobierno en línea – SISAGEL alineado con la norma 27000 para el instituto nacional de formación técnica profesional de la Guajira,” Universidad Nacional, Abierta y a Distancia - UNAD, 2014.

[76] D. Espinosa T, J. Martínez P, and S. Amador D, “Gestion del Riesgo en la Seguridad de la Información Base en la Norma ISO/IEC 27005 de 2011, proponiendo una Adaptación de la Metología Octave-s. Caso de Estudio: Proceso de Inscripciones y Adminisiones en la División de Admisión Registro y Control Académ,” Universidad del Cauca, 2014.

[77] ISO27k Forum and IsecT Ltd., “Toolkit ISO27k.” [Online]. Available: http://www.iso27001security.com/html/toolkit.html. [Accessed: 20-Jan-2017].

[78] Universidad del Cauca, “Elaboración y Control de Documentos,” 2016. [Online]. Available: http://facultades.unicauca.edu.co/prlvmen/sites/default/files/procesos/PE-GS-2.2.1-PR-1 Elaboraci%C3%B3n y Control de Documentos_0.pdf. [Accessed: 24-Apr-2017].

[79] D. Espinosa T, J. Martínez P, and S. Amador D, “Anexos - Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metodología OCTAVE-S.” 2014.

[80] Universidad del Cauca, “Resolución R-785 de 2015 - Política del Sistema de Gestión de Seguridad de la Información de la Universidad del Cauca,” 2015. [Online]. Available: http://www.unicauca.edu.co/versionP/documentos/resoluciones/resoluci%C3%B3n-r-785-de-2015-sistema-de-seguridad-de-la-informaci%C3%B3n-de-la-universidad-del-cauca. [Accessed: 25-Apr-2017].

[81] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, *Guia de implementacion OCTAVE. Versión 1.0*. 2005, pp. 1–970.

[82] D. Espinosa T, J. Martínez P, and S. Amador D, “Artículo - Gestión del Riesgo en la Seguridad de la Información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S. Caso de Estudio: Proceso de Inscripciones y Admisiones en la División de Admisión Registro y,” *USBMed*, vol. 5, no. 2, pp. 33–43, 2014.

[83] MinTIC Colombia., *Modelo de Seguridad y Privacidad de la Información*. MSPI, 2016.

[84] M. Wilson and J. Hash, *Building an Information Technology Security Awareness and Training Program*. NIST SP 800-50, 2003.

[85] European Foundation for Quality Management, *Modelo EFQM de excelencia*. 2013.

[86] Club Excelencia en Gestión, “Resumen del VI Encuentro del club de directores de calidad e innovación.”

[87] A. Rayme Serrano, “Gestión de seguridad de la información y los servicios críticos de las universidades : un estudio de tres casos en Lima Metropolitana,” Universidad Nacional Mayor de Dan Marcos, 2007.

[88] A. Pulido Barreto and J. Martinez Rodriguez, “Modelo para la implementación del sistema general de seguridad informatica y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático.,” Universidad Nacional, Abierta y a Dstancia, 2016.

[89] O. Sierra Jaramillo, “Estudio de los procesos de seguridad de la información digital en las empresas del departamento de Risaralda.,” Universidad Tenologia de Pereira, 2011.

[90] J. Pineda, “Encuesta De Seguridad De La Información En Universidades Ecuatorianas Miembros De Cedia ”,” 2014.

[91] M. . Á. Cea D’Ancona, “Metodología Cuantitativa: estrategias y técnicas de la investigación social,” *Metodol. cuantitativa estrategias y técnicas Investig. Soc.*, p. 168, 1998.

[92] GMV Innovating Solutions, “Implantación de SGSI en una empresa española. Experiencia Practica.”