GESTIÓN Y CREACIÓN DEL PLAN DE EJECUCIÓN DEL PROCESO PARA EL PROYECTO DE CERTIFICACIÓN CON LA NORMA ISO 27001:2005 EN LA FCV

SILVIA MARGARITA DIAZ DIAZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD INGENIERÍAS FÍSICO MECÁNICAS
ESCUELA INGENIERÍA DE SISTEMAS
BUCARAMANGA
2012

GESTIÓN Y CREACIÓN DEL PLAN DE EJECUCIÓN DEL PROCESO PARA EL PROYECTO DE CERTIFICACIÓN CON LA NORMA ISO 27001:2005 EN LA FCV

SILVIA MARGARITA DIAZ DIAZ

Trabajo de grado para optar por el título de Ingeniera de Sistemas

Director
PEDRO JAVIER TRUJILLO TARAZONA
Magíster en Informática
Docente Cátedra de la Escuela de Ingeniería de Sistemas
Universidad Industrial de Santander

Tutor
JAIDER FERNANDO RODRÍGUEZ LOZANO
Ingeniero de Sistemas
Jefe del Departamento Tecnología Informática
Fundación Cardiovascular de Colombia

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO MECÁNICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2012

A Matilde, Margarita, Fabio, Natalia y Luis

AGRADECIMIENTOS

La autora expresa sus agradecimientos a:

Su familia por su apoyo incondicional.

La Universidad Industrial de Santander y la Escuela de Ingeniería de Sistemas por su formación académica, cultural, profesional e integral.

La Fundación Cardiovascular de Colombia, por su aporte en el desarrollo del presente Proyecto de Grado y disponer los recursos para realizar la práctica empresarial en la entidad.

El profesor Pedro Javier Trujillo, por sus aportes, disposición y apoyo a lo largo de la realización del Proyecto.

El Dr. Gilberto Reyes, por permitir llevar a cabo mi proyecto de grado en la Dirección de Tecnología Informática.

El Ingeniero Jaider Fernando Rodríguez, por su dedicación y guía en el desarrollo de la práctica.

La Ingeniera Leidy Viviana Ortiz, por su constante apoyo, disposición y aprecio brindado. A todo el personal de la Dirección de Tecnología Informática por su gran compañerismo y amabilidad.

CONTENIDO

Pág.

INTRODUCCIÓN 21
1. DESCRIPCIÓN DE LA PRÁCTICA 23
1.1. JUSTIFICACIÓN 23
1.2. DEFINICIÓN DEL PROBLEMA 24
1.3. OBJETIVO GENERAL 25
1.4. OBJETIVOS ESPECÍFICOS 26
1.5. IMPACTO 26
1.6. METODOLOGÍA DE LA PRÁCTICA EMPRESARIAL 28
2. FUNDACIÓN CARDIOVASCULAR DE COLOMBIA 30
2.1. ESTRUCTURA ORGANIZACIONAL 30
2.1.1. Misión 32
2.1.2. Visión 32
2.2. RECONOCIMIENTOS Y CERTIFICACIONES 32
2.3. DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA 33
2.3.1. Organigrama 34
3. MARCO TEÓRICO 35
3.1. SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN 35
3.1.1. Seguridad de información 35
3.1.2. ¿Por qué es importante un SGSI? 37
3.1.3. Documentación de un SGSI 37
3.2. ISO 27001:2005 40
3.2.1. Preliminar: Serie 27000 40
3.2.2. Proceso de implementación 41
3.2.3. Gestión de riesgos 44
3.2.4. Estructura y cláusulas 45
4. PLAN DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN BASE A LA ISO 27001:2005 47
4.1. OBJETIVOS DEL PLAN DE IMPLEMENTACIÓN 48

4.1.1. Objetivos específicos 48
4.2. JUSTIFICACIÓN 48
4.3. RESPONSABILIDADES 49
4.4. METODOLOGÍA DE IMPLANTACIÓN 50
4.5. FASE 1: ANÁLISIS DE LA SITUACIÓN ACTUAL 51
4.5.1. Identificar información relevante 51
4.5.2. Definir el alcance del sistema 52
4.5.3. Identificación de los activos de información 54
4.5.4. Análisis de brecha 56
4.6. FASE 2: ANÁLISIS Y GESTIÓN DE RIESGOS - METODOLOGÍA 57
4.6.1. Introducción a la metodología de gestión de riesgo 58
4.6.1.1. Objetivos gestión de riesgo 59
4.6.2. Identificación de amenazas y vulnerabilidades 60
4.6.3. Análisis de riesgo 64
4.6.4. Evaluación del riesgo 66
4.6.4.1. Cálculo del riesgo 67
4.6.4.2. Mapa de riesgos 67
4.6.5. Tratamiento del riesgo 70
4.6.6. Riesgo residual 72
4.7. FASE 3: ESTABLECIMIENTO Y DIVULGACIÓN DEL SGSI 73
4.7.1. Políticas y objetivos de seguridad de información 73
4.7.2. Elaboración de la Declaración de Aplicabilidad 75
4.7.3. Registro de documentos de seguridad 76
4.7.4. Elaboración procedimientos de gestión 76
4.7.5. Hitos 77
4.8. FASE 4: IMPLANTACIÓN DEL SGSI 77
4.8.1. Plan de tratamiento de riesgos 77
4.8.2. Planes de formación y concientización 78
4.8.3. Implementar los controles 80
4.9. FASE 5: CONTROL Y SUPERVISIÓN DEL SGSI 80
4.9.1. Detectar errores en la implementación de los controles 80

4.9.2. Detectar y registrar eventos e incidentes de seguridad 81
4.9.3. Revisar los riesgos 81
4.9.4. Auditorías internas 82
4.10. FASE 6: MANTENIMIENTO Y MEJORA DEL SGSI 82
5. PROYECTO DE IMPLEMENTACIÓN DE UN SGSI EN LA DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA DE LA FCV 84
5.1. RESPONSABILIDADES 84
5.2. ANÁLISIS DE LA SITUACIÓN ACTUAL – FASE UNO 85
5.2.1. Información relevante de la Dirección 85
5.2.2. Delimitación del alcance del SGSI 85
5.2.3. Registro de activos de información 90
5.2.4. Brecha existente 91
5.3. INFORME DE LA GESTIÓN DE RIESGOS – FASE DOS 95
5.4. DIVULGACIÓN DEL SISTEMA – FASE TRES 100
5.4.1. Contenido del manual de políticas de seguridad 100
5.4.2. Objetivos del SGSI 101
5.3.3. Declaración de Aplicabilidad 102
5.4. IMPLEMENTACIÓN DE LOS CONTROLES – FASE CUATRO 102
5.4.1. Plan de tratamiento de riesgo 102
5.4.2. Planes de formación y concientización 103
5.4.3. Implantación de los controles 106
5.5. CONTROL Y MEJORA CONTINUA DEL SISTEMA 107
6. PIRÁMIDE DOCUMENTAL DEL SGSI EN LA DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA 109
6.1. NIVELES DE LA DOCUMENTACIÓN 109
6.2. RELACIÓN Y REQUISITOS 111
6.2.1. Evidencias del proceso de implementación 112
6.2.2. Requisitos de la ISO 27001:2005 112
7. RESULTADOS 113
7.1. RESULTADOS POR FASES 113
7.1.1. Evidencias de los controles implementados (documentación) 116
7.2. APORTES A LA DTI Y A LA EMPRESA 117

7.2.1. Hallazgos 117
RECOMENDACIONES 120
CONCLUSIONES 122
BIBLIOGRAFÍA 124
ANEXOS 127

LISTA DE TABLAS

Tabla 1. Certificados ISO 27001 en Colombia 27
Tabla 2. Organizaciones registradas en IQNet certificadas con ISO 27001 28
Tabla 3. Unidades Estratégicas de Negocio FCV 30
Tabla 4. Acreditaciones, certificaciones, reconocimientos y premios FCV 32
Tabla 5. Propiedades de la información 36
Tabla 6. Contenido del manual de seguridad 38
Tabla 7. Serie 27000 40
Tabla 8. Contenido de la ISO 27001:2005 46
Tabla 9. Etapas metodología proceso de implementación 50
Tabla 10. Lineamientos de clasificación para activos de información 54
Tabla 11. Clasificación amenazas 61
Tabla 12. Clasificación vulnerabilidades 62
Tabla 13. Valor de los factores de riesgo por criterio: probabilidad de ocurrencia. 64
Tabla 14. Valor de los factores de riesgo por criterio: impacto 65
Tabla 15. Nivel de criticidad del riesgo (criterios para la aceptación) 65
Tabla 16. Niveles de riesgo 66
Tabla 17. Nivel de prioridad del activo de información 68
Tabla 18. Niveles de exposición 69
Tabla 19. Grado de peligrosidad 69
Tabla 20. Criterios para las opciones de tratamiento de riesgo 72
Tabla 21. Implementación de controles 91
Tabla 22. Número de controles por nivel de implementación 92
Tabla 23. Frecuencia niveles de riesgo 96
Tabla 24. Porcentaje amenazas por tipo 97
Tabla 25. Proceso formación y concientización 103
Tabla 26. Contenidos para divulgación del SGSI 105
Tabla 27. Indicadores de eficacia 108
Tabla 28. Identificación de documentos 112

Tabla 29. Resultados y avances proceso implantación SGSI - ISO 27001 114

LISTA DE FIGURAS

Figura 1. Organigrama Corporativo 31
Figura 2. Estructura de la Dirección de Tecnología Informática.....34
Figura 3. Pirámide documental 38
Figura 4. Modelo PHVA aplicado a los procesos SGSI 42
Figura 5. Diagrama de elipses de la interacción entre procesos 53
Figura 6. Conceptos base para gestión de riesgos.....59
Figura 7. Relación causa-probabilidad-efecto entre componentes de la gestión de riesgos.....59
Figura 8. Diagrama de flujo opciones de tratamiento de riesgo.....72
Figura 9. Aspectos de la redacción de políticas de seguridad de información.....74
Figura 10. Requisitos de una política de seguridad de información.....75
Figura 11. Objetivos de los planes de formación y concientización 79
Figura 12. Número de controles implementados 92
Figura 13. Número de controles por categoría 94
Figura 14. Ejemplo tasación de un activo de información: Servidor de datos.....96
Figura 15. Actividades de formación y concientización.....105
Figura 16. Mecanismos de monitoreo y control 106
Figura 17. Pirámide documental DTI 109
Figura 18. Modelo del proceso de implementación del SGSI 116

GLOSARIO

ACTIVO DE INFORMACIÓN: Se refiere a toda pertenencia de una organización que tiene gran importancia para ella y sus operaciones.

AMENAZA: Es un factor que puede explotar una vulnerabilidad y generar un evento o incidente de seguridad.

ANÁLISIS DE RIESGO: Proceso mediante el cual se identifican las amenazas y vulnerabilidades que pueden producir un riesgo, y las relaciones entre ellas.

CLÁUSULA: Establece los lineamientos y acciones generales para cumplir con las exigencias de la ISO 27001:2005.

CONFIDENCIALIDAD: Es la propiedad de la información que implica que no sea revelada o manipulada por personas o procesos no autorizados.

CONTROL: Aspectos de la gestión de seguridad de información que dan apoyo para las acciones de implementación para la reducción del riesgo.

DECLARACIÓN DE APLICABILIDAD: Contiene los objetivos de control y controles contemplados en la norma ISO 27001 por el SGSI, basándose en la evaluación de riesgos, teniendo en cuenta la razón de inclusiones y exclusiones.

DISPONIBILIDAD: Es el atributo de la información que consiste en que esté al alcance de todo proceso o persona que lo requiera en el momento indicado.

PROPIETARIO DEL ACTIVO DE INFORMACIÓN: Persona o cargo que tiene la responsabilidad del control, desarrollo, uso, mantenimiento y seguridad de un activo. No significa que tenga algún derecho de propiedad sobre el mismo.

EVALUACIÓN DEL RIESGO: Valoración y cálculo de las probabilidades de ocurrencia de las amenazas que originan el riesgo, junto con el factor hallado en la tasación de activos de información.

EVENTO DE SEGURIDAD: Cuando se presenta una falla de seguridad de cualquier tipo (tecnológico, organizacional, biológico, etc.).

GESTIÓN DEL RIESGO: Indica todo el proceso mediante el cual se identifican, valoran y calculan los riesgos, para encontrar, asignar e implementar la solución más eficiente (tratamiento de riesgos).

GRUPO PRIMARIO: Equipo de trabajo compuesto por un líder y sus colaboradores se reúnen periódicamente para buscar una mayor eficacia en sus tareas, exponer resultados de cada área y se presentar inquietudes y mejoras.

IMPACTO: Factor del riesgo que indica el nivel del daño que puede causar en las actividades y el negocio en caso de que ocurra.

INCIDENTE DE SEGURIDAD: Es cuando se presenta una serie de eventos de seguridad que pueden comprometer la continuidad del negocio y tener un alto impacto en éste.

INTEGRIDAD: Propiedad o atributo de la información que implica su exactitud y no corrupción.

ISO 27001:2005: Estándar internacional para la seguridad de información. La certificación con esta norma implica una auditoría que rectifica la implantación real y eficiencia del Sistema de Gestión de Seguridad de Información.

MANUAL DE SEGURIDAD: Documento de la pirámide documental de un sistema de gestión, que permite establecer las directrices que administran el sistema.

METODOLOGÍA DE IMPLEMENTACIÓN: Indica el proceso a seguir para implementar un SGSI, compuesto por 6 fases.

METODOLOGÍA GESTIÓN DE RIESGO: Describe el proceso para gestionar los riesgos sobre los activos de información con base en los requerimientos de la norma.

METODOLOGÍA PRÁCTICA EMPRESARIAL: El proceso que se llevó a cabo para el desarrollo de este proyecto de grado.

OBJETIVO DE CONTROL: Propósito de un grupo de controles de acuerdo al aspecto organizacional que abarca.

PIRÁMIDE DOCUMENTAL: Es la base que representa los niveles de la documentación y funcionamiento de un sistema de gestión.

PLANIFICAR, HACER, VERIFICAR, ACTUAR: Es la metodología utilizada para el proceso de implementación de los sistemas de gestión.

PROBABILIDAD DE OCURRENCIA: Es el factor del riesgo que indica la probabilidad de que ocurra.

RIESGO: Es la probabilidad de que una amenaza explote una vulnerabilidad. Se compone de dos factores: la probabilidad de ocurrencia y el impacto al negocio.

SEGURIDAD DE INFORMACIÓN: Consiste en la protección de la confidencialidad, integridad y confidencialidad de la información. No se limita al aseguramiento de las tecnologías informáticas, ya que tiene en cuenta recursos humanos, obligaciones legales, espacios físicos y áreas de trabajo.

SEGURIDAD INFORMÁTICA: Se enfoca en la protección de la infraestructura tecnológica y computacional. Comprende software, hardware, bases de datos, archivos, etc.

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN: Sistema de gestión que se basa en el análisis de riesgos, estructuración de procesos, creación de políticas y responsabilidades con el fin de proteger los activos de información.

TASACIÓN DE ACTIVOS DE INFORMACIÓN: Proceso mediante el cual se define y calculan los valores de disponibilidad, integridad y confidencialidad que son requeridos (ideales) por cada activo de información.

TRATAMIENTO DE RIESGOS: Es el proceso mediante el cual se seleccionan las opciones mediante las cuales se le dará tratamiento a los riesgos calculados.

UNIDAD ESTRATÉGICA DE NEGOCIO: Conjunto de actividades homogéneo desde el punto de vista estratégico, que permite formular una estrategia común pero a la vez diferente para otras actividades del negocio.

VULNERABILIDAD: Es una debilidad del sistema o de la empresa frente a la seguridad de información. Puede ser aprovechada por una amenaza y generar un evento de seguridad (riesgo).

LISTADO DE SIGLAS

CRM: Customer Relationship Management.

CTE: Centro Tecnológico Empresarial.

DdA: Declaración de Aplicabilidad.

DTI: Dirección de Tecnología Informática.

ERP: Enterprise Resource Planning.

FCV: Fundación Cardiovascular de Colombia.

ICONTEC: Instituto Colombiano de Normas Técnicas y Certificación.

ISMS: Information Security Management System.

IQNet: International Certification Network.

PHVA: Planificar, Hacer, Verificar y Actuar.

PTR: Plan de Tratamiento de Riesgo.

SGC: Sistema de Gestión de Calidad

SGSI: Sistema de Gestión de Seguridad de Información.

UEN: Unidad Estratégica de Negocio.

RESUMEN

TÍTULO: GESTIÓN Y CREACIÓN DEL PLAN DE EJECUCIÓN DEL PROCESO PARA EL PROYECTO DE CERTIFICACIÓN CON LA NORMA ISO 27001:2005 EN LA FCV*

AUTOR: DIAZ DIAZ, Silvia Margarita**

PALABRAS CLAVES: Sistema de Gestión de Seguridad de Información. ISO 27001:2005. Activos de información. Riesgos. Amenazas y vulnerabilidades. Fundación Cardiovascular de Colombia. Dirección de Tecnología Informática (DTI). Declaración de Aplicabilidad. Pirámide documental.

DESCRIPCIÓN: La Dirección de Tecnología Informática de la Fundación Cardiovascular de Colombia ha establecido en sus objetivos estratégicos avanzar en el proceso de gestión de seguridad de información. Los aportes brindados por medio de la práctica empresarial permitieron generar un mayor nivel de conformidad a la ISO 27001:2005, y por tanto avanzar en el proyecto de certificación. En el desarrollo de este proyecto de grado se creó un plan para implementar un SGSI en la Dirección de Tecnología Informática, en base a los procesos y actividades que se llevan a cabo en esta y en la FCV.

Como resultado de la práctica, se generó el plan de implementación para la DTI, que comprende la identificación de los procesos, el desarrollo de la metodología para la ISO 27001:2005 y su aplicación en la DTI; reflejándose en la definición de información relevante, el alcance del SGSI, el mapa de riesgos, la Declaración de Aplicabilidad y la pirámide documental, entre otros. Se generó así la base y los documentos que sirvieron de apoyo para el SGSI de la DTI, los cuales reposan en dicha Dirección. Se logró también la sensibilización y socialización de la importancia de la Seguridad de la Información al interior de la DTI, y finalmente, la implementación de los controles establecidos por la norma.

Este plan de implementación permitió igualmente a la DTI, cumplir con su plan de acción de 2011 (Diagnóstico de cumplimiento de la DTI frente a la ISO 27001:2005, mapa de riesgos, inventario de activos de información).

---

* Trabajo de Grado, Práctica Empresarial

** Facultad de Ingenierías Físico Mecánicas. Escuela de Ingeniería de Sistemas e Informática. Director de Proyecto: M.Sc. en Informática Pedro Javier Trujillo Tarazona. Tutor: Ingeniero de Sistemas Jaider Fernando Rodriguez

ABSTRACT

TITLE: MANAGEMENT AND CREATION OF THE IMPLEMENTATION FOR THE DESIGN PROCESS FOR THE CERTIFICATION WITH ISO 27001:2005 AT FCV [*]

AUTHOR: DIAZ DIAZ, Silvia Margarita[**]

KEYWORDS: Information Security Management System (ISMS). ISO 27001:2005. Information assets. Risks. Threats and vulnerabilities. Cardiovascular Foundation of Colombia. Information Technology Division (ITD). Statement of Applicability. Documental pyramid.

DESCRIPTION: The Information Technology Division of Cardiovascular Foundation of Colombia has established in its strategic objectives, advancing and leading the process of security information management. Contributions provided through the business practice allowed to generate a better conformity level to ISO 27001:2005, and therefore to progress in the certification project. In the development of this Graduation Work, it was created a plan to implement ISMS at Information Technology Division, based on activities and process that are carried out at it and at FCV.

As a result of this practice, it was created the implementation plan for ITD, which includes the identification of processes, a methodology development for ISO 27001:2005 and its application in ITD; reflecting itself in the definition of relevant information, ISMS' scope, risk management, Statement of Applicability and documental pyramid, inter alia. It was generated a basis and the documentation that supported the creation of an ISMS in ITD, which lie in its domains. It was also accomplished the socialization and sensitization of the information security importance inside ITD, and finally, the implementation of the controls established by the standard.

This implementation plan also allowed ITD to fulfill its 2011 action plan (Accomplishment diagnosis of ITD with ISO 27001, risk map, information asset inventory).

---

* Engineer Graduation Work, Business Practice

** Faculty of Physical and Mechanical Engineering. School of System Engineering. Project Director: Mg. on Computer Science Pedro Javier Trujillo Tarazona. Tutor: System Engineer Jaider Fernando Rodríguez.

INTRODUCCIÓN

La información es un bien de pertenencia única para una empresa. Esto quiere decir que no debe estar al alcance de procesos o personas no interesadas y debe lograr los niveles más altos posibles de confidencialidad, disponibilidad e integridad. Es fundamental evitar que dicha información resulte en manos equivocadas que puedan darle mal uso, utilizándola para fines que dañen la integridad de la empresa. La ISO 27001:2005 se plantea como el estándar internacional que establece las pautas para implementar un Sistema de Gestión de Seguridad de la Información.

Dado que la Fundación Cardiovascular de Colombia es una empresa en auge y de constante crecimiento, la gestión de la seguridad de información le permitirá manejar adecuadamente los grandes volúmenes de información que fluyen en sus procesos, protegiendo aquello por lo que se ha diferenciado. La Dirección de Tecnología Informática, como principal responsable por el procesamiento y almacenamiento de la información, tiene como objetivo estratégico certificarse con la ISO 27001:2005; pero para llevarlo a cabo se debe gestionar el proceso, ya que requiere tiempo, estudio sobre el tema y dedicación.

Bajo estas necesidades, se busca crear un plan de implementación del Sistema de Gestión de Seguridad de Información en la Dirección de Tecnología Informática de la Fundación Cardiovascular de Colombia, ya que cada vez se ve más necesaria la certificación con la ISO 27001:2005 y la inversión a la seguridad de información, y una buena planificación encamina a una buena implementación y el éxito del proceso.

En el primer capítulo de este libro se presentan las especificaciones del proyecto como práctica empresarial.

El capítulo dos describe a la Fundación Cardiovascular de Colombia y a la Dirección de Tecnología Informática.

En el capítulo tres se enfoca al lector en la temática por medio de un marco teórico que presenta las características y procesos de un SGSI y la ISO 27001:2005.

El capítulo cuatro contiene el producto del proyecto de grado, describe el proceso para implementar un SGSI en cualquier Área, Dirección o UEN de la FCV, en base a la vivencia de la práctica empresarial en la Dirección de Tecnología Informática.

En el quinto capítulo se presentan los resultados de aplicar el proceso descrito en el capítulo cuatro en la Dirección de Tecnología Informática, bajo la metodología descrita.

Finalmente el capítulo seis presenta la pirámide documental elaborada para la Dirección de Tecnología Informática, con los resultados de la documentación exigida por la ISO 27001:2005.

1. DESCRIPCIÓN DE LA PRÁCTICA

1.1. JUSTIFICACIÓN

La Práctica Empresarial como Proyecto de Grado para obtener el título de Ingeniera de Sistemas, no sólo permite a la estudiante aplicar sus conocimientos y ejecutar las habilidades adquiridas en la carrera; sino que también da paso al desarrollo profesional de la estudiante, teniendo contacto directo con una empresa que permite vivir una experiencia laboral, social y académica del mundo real al que se enfrentará al lograr la titulación.

Se establece el primer vínculo con la vida profesional, en la cual se encaran los desafíos y se plantea el enfoque mediante el cual la estudiante se desenvolverá los años siguientes en el ejercicio de la profesión.

La Escuela de Ingeniería de Sistemas e Informática - EISI se verá beneficiada con este proyecto en la medida en que se promueve el futuro profesional de los estudiantes, el vínculo empresarial, el desarrollo de un perfil profesional propio basado en las características de un Ingeniero de Sistemas UIS y el hallazgo de la orientación e intereses profesionales del futuro egresado. También se permitirá la divulgación al interior de la EISI de la norma ISO 27001:2005 y su importancia en las organizaciones.

Para la empresa, la practicante será un apoyo en el proceso de implantación de un Sistema de Gestión de Seguridad de Información a favor de la obtención de la certificación ISO 27001:2005, lo que le permitirá ingresar a otro nivel organizacional, proteger su información y obtener ventaja competitiva. Este proceso es muy importante para la Dirección de Tecnología Informática de la Fundación Cardiovascular de Colombia, pues establecer las pautas y el plan de

ejecución del proyecto para lograr ésta certificación significa un gran paso en el manejo de riesgos, seguridad de la información, control organizacional y otros aspectos que brinda la implementación del SGSI.

Vale destacar que realizar la práctica empresarial en una organización de gran importancia en el sector salud, para la operación de doce unidades de negocio (entre ellas la Zona Franca: “Hospital Internacional”) y para el desarrollo de grandes proyectos tecnológicos a nivel nacional; es una gran oportunidad para la autora del este proyecto y el buen nombre de la Escuela de Ingeniería de Sistemas.

1.2. DEFINICIÓN DEL PROBLEMA

Las empresas hoy día manipulan, almacenan y procesan su información y datos a través de sus sistemas de información, aplicaciones, bases de datos, redes de comunicaciones y otros medios de procesamiento. Debido a que la información es de suma importancia para una compañía, está constantemente expuesta a amenazas externas y vulnerabilidades dentro de la organización.

¿Qué sucede si la empresa no está preparada para actuar frente a estos eventos, que pueden llegar a tener un impacto catastrófico? La pro actividad es un factor clave. Muchas organizaciones están acostumbradas a contar con planes de contingencia para reaccionar ante incidentes informáticos, ¿pero realmente están protegiendo su información, o actúan conforme se presentan eventos? Las consecuencias de un incidente pueden llegar a ser catastróficas, más aún cuando no hay acciones que disminuyan el impacto de un riesgo.

La Fundación Cardiovascular de Colombia es una gran empresa[1], certificada actualmente con la norma ISO 9001:2000 de Sistemas de Gestión de Calidad (sistema para garantizar la excelencia de sus servicios, promover una cultura de calidad y responsabilidad y lograr una mejora continua en la gestión de calidad).

Un objetivo estratégico de la Dirección de Tecnología Informática definido en el plan de acción de 2011 es fortalecer los sistemas de información, de lo cual se desprende un objetivo específico que es garantizar la seguridad informática. Para avanzar en el proceso y lograr la certificación con la ISO 27001:2005, se estipularon una serie de actividades clave para cumplir el objetivo específico, y que se definieron como la Fase 1 de la ISO 27001:

- Diagnóstico del cumplimiento de la Fundación Cardiovascular de Colombia frente a los requisitos de la ISO 27001:2005.
- Construcción del Mapa de Riesgos informáticos en el Sistema de Gestión de Seguridad de Información.
- Inventario de Activos de Información.

Las actividades se cumplieron en su totalidad con la labor realizada por la practicante, cumpliendo con el propósito de esta práctica empresarial. Para el año 2012 las actividades están enfocadas a la obtención del certificado ISO 27001:2005 para los procesos de la Dirección de Tecnología Informática.

1.3. OBJETIVO GENERAL

Definir el modelo de la norma ISO 27001:2005 para aplicar en la Fundación Cardiovascular de Colombia.

1 Gran Empresa: Clasificación de las empresas según su tamaño, con más de 250 trabajadores. [Consultado 10 Julio 2011]. Disponible en <http://www.encolombia.com/economia/Definicionyclasificaciondelaempresa.htm>.

1.4. OBJETIVOS ESPECÍFICOS

- Elaborar una metodología de implantación del SGSI en la empresa acorde a las cláusulas, objetivos de control y controles establecidos en la norma ISO 27001:2005.

- Definir los procesos pertinentes y relevantes a las actividades de negocio e información de la FCV para efectos de definir el alcance del Sistema de Gestión de Seguridad de Información (SGSI) y para realizar análisis de riesgos.

- Desarrollar la Declaración de Aplicabilidad como apoyo en la elaboración del Manual de Seguridad.

- Diseñar la pirámide documental[2] de FCV de acuerdo a las exigencias de la norma identificando los niveles y contenido de la misma.

1.5. IMPACTO

Para gestionar la seguridad de información en una empresa se puede comenzar por implementar un SGSI a la luz de la ISO 27001:2005. Aunque implantar un SGSI no implica la certificación inmediata del estándar (de hecho, muchas empresas se basan en la norma para generar altos niveles de seguridad de la información, más no tienen la certificación como prioridad), es un gran paso para proteger los activos de información más vulnerables.

Se espera un impacto positivo para la FCV, pues aportar para que la empresa cuente con una base que ayude a gestionar el proceso para la certificación ISO

2 ALEXANDER, Alberto G. Diseño de un Sistema de Gestión de Seguridad de Información : Óptica ISO 27001:2005. Primera edición. Bogotá D.C. : Alfaomega Colombiana S.A., 2007. Pirámide Documental, Gráfico 5.1. p 96.

27001:2005 y establezca los fundamentos para una cultura organizacional de seguridad de información, es un logro muy importante.

No sólo se espera un efecto positivo en la FCV, sino también en la Escuela de Ingeniería de Sistemas e Informática (EISI), la cual se verá beneficiada por la divulgación de la norma permitiendo el conocimiento de la misma, su importancia y sus aspectos más esenciales.

Para contextualizar el estado del estándar en el país, en la Tabla 1 se enunciarán las empresas en Colombia que cuentan con un certificado ISO 27001:2005. Además, en la red IQNet se encuentra un registro de otras empresas certificadas por el ICONTEC (Ver Tabla 2).

Tabla 1. Certificados ISO 27001 en Colombia

Nombre	Número de Certificado	Entidad Certificadora	Campo de acción
ACH Colombia S.A.	IS 518175	--	Financiero
ComBanc S.A.	IS 531192	--	Financiero
DIGISOC S.A.S	CO10/3734	SGS Colombia S.A.	Seguridad de información
Etek International Holding Corp.	IS 84320	--	Seguridad de información
Financial Systems Company Ltda	IND92101	Bureau Veritas Certification	Financiero
FLUID SIGNAL GROUP S.A	IND10.2249	Bureau Veritas Certification	Seguridad informática
Ricoh Colombia, S.A.	IS 85241	--	Tecnología
SETECSA S.A	IND102074	Bureau Veritas Certification	Seguridad de información
TELMEX COLOMBIA S.A	IND11.2516U/3	Bureau Veritas Certification	Telecomunicaciones
UNE EPM Telecomunicaciones. S.A E.S.P	IND92122	Bureau Veritas Certification	Telecomunicaciones
UNISYS Global Outsourcing & Infrastructure Services (GOIS)/Maintenance Support Services (MSS)	IS 97104	--	Tecnologías de información

Fuente: *International Register o ISMS Certificates*[3]

3 INTERNATIONAL REGISTER OF ISMS CERTIFICATES. En: Certificate Register. [En línea]. [Consultado 20 de Julio 2011]. Disponible en <http://www.iso27001certificates.com/>

Tabla 2. Organizaciones registradas en IQNet certificadas con ISO 27001

Nombre	Número de Certificado - IQNet	Entidad Certificadora	Principal campo de acción
Asesoría en Sistematización de Datos S.A., ASD S.A	CO-SI009-1	ICONTEC	Tecnologías de información
Banco de la República	CO-SI003-1	ICONTEC	Tecnologías de información
Caja de Compensación Familiar, Compensar S.A.	CO-SI006-1	ICONTEC	Tecnologías de información
Empresa Colombiana de Petróleos, Ecopetrol S.A.	CO-SI007-1	ICONTEC	Transporte, almacenamiento y comunicación
Enlace Operativo	CO-SI005-1	ICONTEC	Tecnologías de información
Jaime Torres C. y Cía. S.A.	CO-SI002-1	ICONTEC	Tecnologías de información
Mareigua LTDA	CO-SI004-2	ICONTEC	Tecnologías de información
Millenium Phone Center S.A.	CO-SI-CER108651	ICONTEC	Transporte, almacenamiento y comunicación
Superintendencia de Sociedades	CO-SI-CER128262	ICONTEC	Administración pública
Ventas y Servicios S.A.	CO-SI-CER134024	ICONTEC	Tecnologías de información

Fuente: IQNET Database of Registered Organisations[4]

En Colombia, todos los Operadores de Información registrados y autorizados por el Ministerio de Protección Social encargados de la liquidación asistida de la Plantilla Integrada de Liquidación de Aportes (PILA), deben estar certificados bajo la ISO 27001:2005, según el Decreto 1931 de 2006[5].

1.6. METODOLOGÍA DE LA PRÁCTICA EMPRESARIAL

La metodología utilizada para el desarrollo de la práctica empresarial corresponde a la de un trabajo analítico y práctico con estudio previo de estándares y normas. Es importante documentarse e informarse sobre la temática de la norma y leerla detenidamente. Los pasos para desarrollar la metodología se representarán por medio de una serie de aspectos cumplidos a lo largo de la práctica en la empresa:

4 IQNET CERTIFICATION NETWORK. En: IQNet Database of Registered Organisations. [En línea]. [Consultado 21 Julio 2011]. Disponible en <http://www.iqnet-certification.com/index.php>

5 PRESIDENCIA DE LA REPÚBLICA. Ministerio de la Protección Social. [En línea]. [Consultado 13 Enero 2012]. Disponible en <http://www.presidencia.gov.co/prensa_new/decretoslinea/2006/junio/12/dec1931120606.pdf>

a. Estudio, revisión, conocimiento y entendimiento de la norma ISO 27001:2005, Gestión de seguridad de información, SGSI, metodologías de implementación y procesos de gestión de calidad de la empresa.

b. Recopilación de la información sobre los procesos de negocio de la empresa y sus actividades:
   - Determinación de procesos críticos y análisis de riesgos a activos.
   - Definición del alcance, objetivos y políticas de seguridad.

c. Creación de un equipo de seguridad de información encargado de la gestión y seguimiento del proceso de implementación del SGSI, conformado por:
   - Jefe de Tecnología Informática
   - Ingeniera Monitor de Calidad DTI
   - Practicante DTI

d. Elaboración del plan de acción del equipo de seguridad de información para la realización del proyecto.

e. Reuniones del equipo (Ingenieros de calidad, Jefe Departamento de Tecnología Informática y Practicante DTI) quincenalmente los viernes a las 4:00 p.m., para el seguimiento del proceso.

f. Se elaboraron tres reportes entregados al director del proyecto, y una reunión con el tutor, el director y la practicante.

g. Se llevarán a cabo una serie de charlas en la UIS y en la FCV sobre las temáticas más importantes del proyecto, para divulgación de la norma en la EISI y otras escuelas, y al Comité de Seguridad de Información en la FCV.

2. FUNDACIÓN CARDIOVASCULAR DE COLOMBIA

La Fundación Cardiovascular de Colombia es una entidad privada sin ánimo de lucro dedicada a prestar servicios de salud de alta calidad. Gracias a la constante dedicación y esfuerzo de sus Directivos y personal, la FCV ha logrado establecerse como una de las clínicas más importantes de Latinoamérica[6]; tanto ofreciendo innovación y calidad en sus productos y servicios como infundiendo valores institucionales.

2.1. ESTRUCTURA ORGANIZACIONAL

Tabla 3. Unidades Estratégicas de Negocio FCV

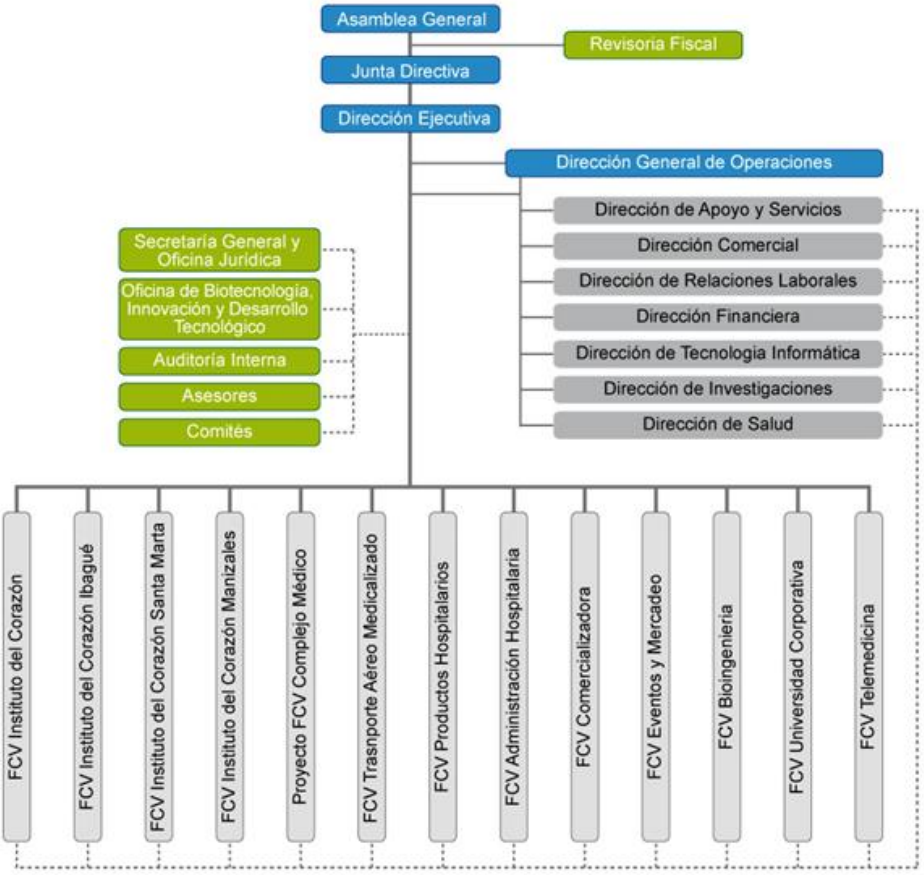
Bioingeniería	Se encarga del diseño, producción y venta de equipos biomédicos, tales como unidades de cuidado intensivo móviles (también para neonatos), electrocardiógrafos, monitores de signos vitales, entre otros.
Telemedicina	Ofrece medicina especializada a regiones de difícil acceso que requieren estos servicios: Tele-consulta, Apoyo diagnóstico (RX: placas – EKG: electrocardiogramas) y Tele-UCI.
Comercializadora	Se dedica a la comercialización (importación y distribución nacional) de insumos, equipos médicos y medicamentos en base a las necesidades de la FCV
Universidad Corporativa	Organiza los convenios y alianzas con reconocidas universidades e instituciones hospitalarias; ofreciendo actividades académicas (capacitaciones, simposios, congresos) para el personal médico, asistencial y administrativo de la FCV
FCV Institutos del Corazón	Entidades prestadoras de servicios médicos cardiovasculares, en neurociencias, trasplantes, hospitalización, especialidades médicas y servicios de apoyo de diagnóstico y terapéutico.
Administración Hospitalaria	Ofrece servicios de operación y administración delegada de IPS (tanto públicas como privadas), bajo un modelo de gestión de alta calidad para mejorar la competitividad y rentabilidad

[6] FUNDACIÓN CARDIOVASCULAR DE COLOMBIA, Noticias. [En línea]. [Consultado 12 de Enero 2012]. Disponible en < http://www.fcv.org/corp/index.php?option=com_content&view=article&id=164:la-fcv-una-de-las-mejores-de-clinicas-de-latinoamerica&catid=41:imagenes-inicio&Itemid=70>

Productos Hospitalarios	Se encarga de la producción y comercialización de insumos médico-quirúrgicos (suturas, ropa quirúrgica desechable, entre otros); y además cuenta con un banco de tejidos
Eventos y Mercadeo	Promueve el deporte y un estilo de vida saludable a través de la planificación, organización y desarrollo de eventos deportivos y culturales, tales como la Maratón de Bucaramanga
Complejo Médico	Se encarga de gestionar el proyecto de la zona franca llamada Hospital Internacional

Fuente: Fundación Cardiovascular de Colombia

Figura 1. Organigrama Corporativo



Fuente: Fundación Cardiovascular de Colombia. Portal de Calidad

2.1.1. Misión

La Fundación Cardiovascular de Colombia es una organización empresarial sin ánimo de lucro, que provee servicios y productos de salud de alta calidad para el desarrollo del sector, buscando permanentemente el bienestar de la comunidad.

2.1.2. Visión

En el año 2020 la Fundación Cardiovascular de Colombia será una organización reconocida a nivel nacional e internacional por la excelencia e innovación de sus productos y servicios orientados principalmente al sector salud.

2.2. RECONOCIMIENTOS Y CERTIFICACIONES

Tabla 4. Acreditaciones, certificaciones, reconocimientos y premios FCV

	Nombre	Entidad	Año	Alcance	Descripción
Acreditaciones	*Quality Approval*	Joint Comission International	2009	Instituto del Corazón Floridablanca	Acreditación internacional, dedicada a la mejora de la calidad y la seguridad en las organizaciones de salud
	Cinco mejores IPS de Colombia	Ministerio de Protección Social	2005	Instituto del Corazón Floridablanca	Reconocida como una de las mejores IPS del país
	Acreditación en salud	ICONTEC	2005	Instituto del Corazón Floridablanca	Acreditación en salud: cumplimiento de estándares de calidad y la atención en salud
			2008		Re acreditación
Certificaciones	Hospital sin Dolor	Asociación Colombiana para el Estudio del Dolor, ACED	2004	FCV	Cumplimiento de los requisitos y procesos necesarios para aliviar el dolor de sus pacientes
			2008		Renovación del certificado
	ISO 9001	BvQi	2001	Instituto del Corazón Floridablanca	Primera IPS en Hispanoamérica
		ICONTEC	2004	FCV	Revisión cumplimiento de los requisitos

			2007	FCV	Renovación del certificado
			2010	FCV	Renovación del certificado bajo la versión ISO 9001:2008
Reconocimientos	Hospital Verde	Nodo de Producción Más Limpia de Santander, UIS, CDMB, CNPML, Secretaria de Salud Departamental y la ANDI	2004	FCV Instituto del Corazón	Categoría de Mejor Desempeño Ambiental
			2006		
			2008	FCV	(Por excelencia). Avances en la gestión ambiental
		UIS, Ministerio de Protección Social, CDMB	2010		(Por excelencia). Gestión adecuada de residuos hospitalarios, sustancias químicas y reducción consumo de agua y energía eléctrica
Premios	Premio Iberoamericano de la Calidad - Reconocimiento Plata	Fundación Iberoamericana de la Calidad FUNDIBEQ	2011	FCV - Instituto del Corazón	Gestión y liderazgo en la calidad de los servicios, basado en el Modelo Iberoamericano de Excelencia en la Gestión

Fuente: Autora, a partir de la Fundación Cardiovascular de Colombia[7]

2.3. DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA

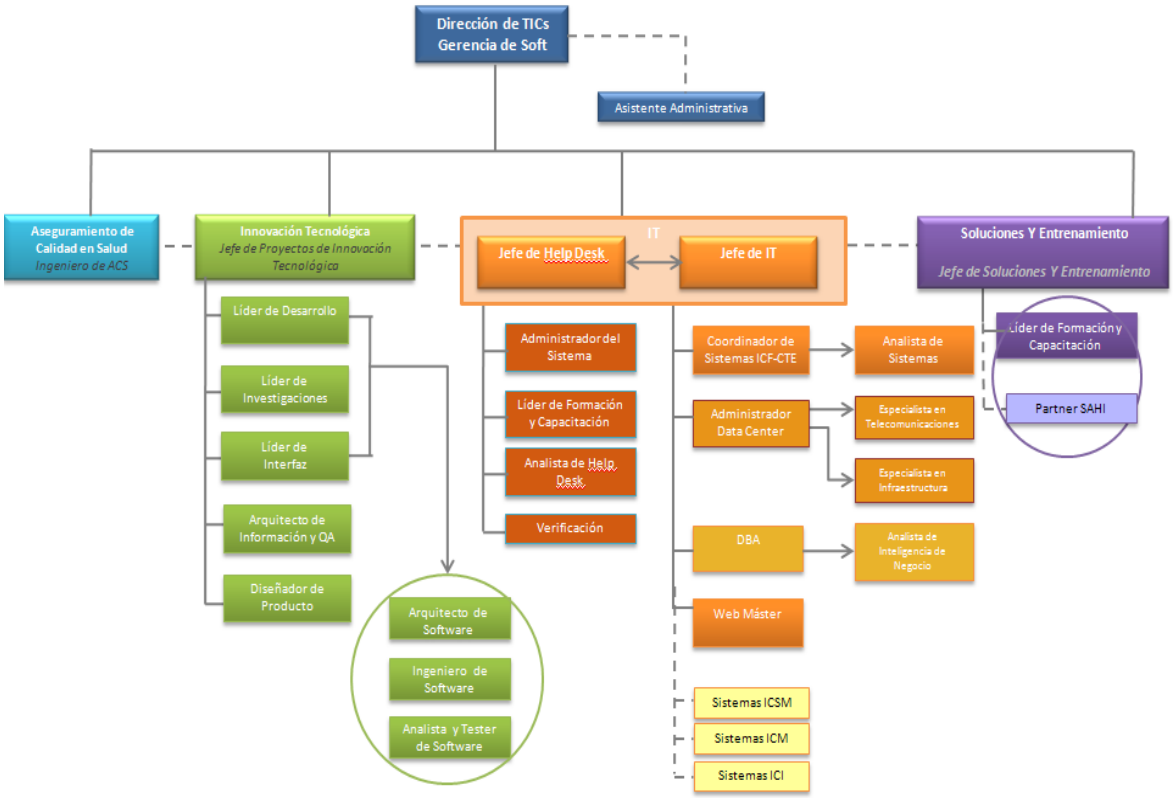
La Dirección de Tecnología Informática hace parte de la Dirección General de Operaciones. Estas Direcciones están conformadas por procesos que son transversales a la organización, con el fin de dar apoyo a las actividades de todas las Unidades Estratégicas de Negocio.

El personal administrativo se encuentra en su mayoría en el Centro Tecnológico Empresarial (CTE), mientras que el personal de apoyo se encuentra en el Instituto del Corazón Floridablanca, así como también en el CTE.

7 FUNDACIÓN CARDIOVASCULAR DE COLOMBIA. En: Acerca de A FCV-ICF, Premios y Reconocimientos. [En línea]. [Consultado 13 Enero 2012]. Disponible en <http://www.fcv.org/ic/index.php?option=com_content&view=article&id=62&Itemid=66&lang=es>

2.3.1. Organigrama

Figura 2. Estructura de la Dirección de Tecnología Informática



Fuente: Dirección de Tecnología Informática, Calidad.

Los principales procesos de la Dirección son:

- Tecnología Informática
- Innovación Tecnológica (Diseño y Desarrollo, Administración de Proyectos)
- Aseguramiento de Calidad
- Soluciones y Entrenamiento

3. MARCO TEÓRICO

3.1. SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

Las organizaciones hoy día deben ser creativas, innovadoras y abiertas al cambio, buscar otros mercados y campos de acción; pero además deben ser cautelosas respecto a las amenazas que pueden afectar el buen funcionamiento del negocio, ya que en un mundo donde la información lo es todo, los ataques tienen como objetivo el robo o divulgación de ella. En este aspecto entra en juego la seguridad de información.

La norma ISO 27001:2005 define al SGSI como la parte del sistema de gestión global, basada en una orientación al riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información[8]. Aunque no es posible alcanzar la seguridad absoluta, el SGSI busca que las empresas gestionen sus riesgos y se conozcan a sí mismas, para así minimizar los ataques a sus activos de información y a su integridad.

3.1.1. Seguridad de información

La seguridad de la información consiste en la preservación de la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas implicados en su tratamiento dentro de una organización[9]. La información de una organización es propiedad de ella, y no debe estar expuesta a terceros, personas o entidades que no la requieran y tengan intereses diferentes.

8 ALEXANDER, Alberto G. Diseño de un Sistema de Gestión de Seguridad de Información : Óptica ISO 27001:2005. Primera edición. Bogotá D.C. : Alfaomega Colombiana S.A., 2007. P 19.

9 ISO 2700. Certificación, SGSI. En: El portal de ISO 27001 en español. [En línea]. [Consultado 9 de Mayo 2011] disponible en < http://www.iso27000.es/sgsi.html#section2a>

Por esta razón, las empresas deben asegurar la continuidad del negocio, disminuyendo el impacto de un riesgo por medio de una estrategia claramente definida y un plan de reanudación operativa. Para lograr la protección de la información y evitar fraudes, fugas y demás amenazas, las organizaciones deben identificar los activos de información imprescindibles, analizar y evaluar los riesgos que mayor impacto tienen en ellos y encontrar la forma de tratarlos.

Tabla 5. Propiedades de la información

Confidencialidad	Es la propiedad de la información que implica que esté disponible y no sea revelada a personas, entidades o procesos no autorizados.
Integridad	Requiere el mantenimiento de la exactitud, completitud y no corrupción de la información y de sus métodos de manejo.
Disponibilidad	Es la propiedad de la información que esté disponible, accesible y utilizable cuando una persona, entidad o proceso la requiera, así como a los sistemas de tratamiento.

Fuente: Portal de la ISO 27001 en español[10]

Activo de información. Según la ISO 27001:2005, es "*cualquier cosa que tenga valor para la organización*"[11]; por lo tanto, un activo de información puede ser un proceso, el recurso humano, los equipos informáticos, software, documentos, imagen corporativa, servicios y por supuesto, la información. Puede decirse entonces que un activo es una propiedad de la organización, tangible o intangible, que es de gran importancia para ella y para sus operaciones.

Es importante recalcar que la correcta identificación de los activos de información en el proceso de establecer el alcance del SGSI es imprescindible, pues si no se

10 ISO 27000. Certificación, SGSI. En: El portal de ISO 27001 en español, Herramientas. [En línea]. [Consultado 9 de Mayo 2011]. Disponible en <http://www.iso27000.es/sgsi.html#section2a>

11 INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Estándar Internacional ISO/IEC 27001 en español. [En línea]. Cláusula 3, 3.1 Activo. [Consultado 2 de Mayo]. Disponible en <http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf>

tiene claro qué es importante y qué se debe custodiar, el proceso se estaría desarrollando sobre una base débil.

3.1.2. ¿Por qué es importante un SGSI?

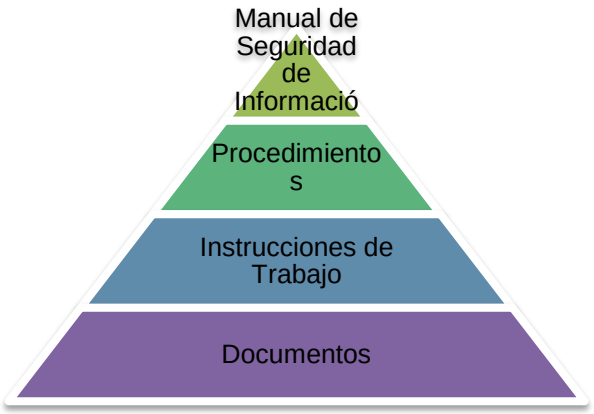
El SGSI permite alcanzar altos niveles de seguridad para proteger los activos de información y gestionar los riesgos más altos. Es una ayuda para la organización para conocerse y monitorear sus objetivos de negocio. De esta manera, la empresa puede conocer los riesgos a los que está sometida su información y manejarlos, revisarlos y mejorar sus planes constantemente.

El modelo de la gestión de la seguridad debe seguir un proceso que incluya una planificación e implantación de una serie de controles de seguridad, contando con la participación activa de todo el personal de la empresa y con la Dirección al mando del proceso.

3.1.3. Documentación de un SGSI

Según la ISO 9001 para Sistemas de Gestión de Calidad, la documentación se representa por medio de cuatro niveles. Esto se puede tomar como base para crear un modelo análogo para un Sistema de Gestión de Seguridad de Información a la luz de la ISO 27001, y es llamada la pirámide documental.

Figura 3. Pirámide documental



Fuente: ALEXANDER, Alberto G. Metodología para la documentación de un SGSI[12]

Manual de seguridad de información. Aunque no es requisito estricto del modelo y no hay cláusula que lo exija, es un gran apoyo dado que facilita la labor de auditoría y agrupa la documentación importante para el inicio y constitución del proceso[13]. Los contenidos que debería abarcar este manual corresponden a la política del SGSI, el alcance, los procedimientos y controles de soporte, la descripción de la metodología de evaluación, reporte y plan del riesgo y la DdA.

Tabla 6. Contenido del manual de seguridad

Alcance del SGSI	Corresponde a la identificación de las dependencias, relaciones y limitaciones.
Políticas y objetivos de seguridad	Establece el compromiso que ha de adquirir la gerencia y el rumbo que tomará la organización para gestionar la seguridad de la información.
Enfoque de evaluación de riesgos	Establece el compromiso que ha de adquirir la gerencia y el rumbo que tomará la organización para gestionar la seguridad de la información.
Plan de tratamiento de riesgos	Identifica las tareas de la gerencia, recursos, prioridades y responsabilidades para gestionar los riesgos, en función de los objetivos de control identificados, la disponibilidad de recursos y los activos.

12 ALEXANDER, Alberto G. Diseño de un Sistema de Gestión de Seguridad de Información : Óptica ISO 27001:2005. Primera edición. Bogotá D.C. : Alfaomega Colombiana S.A., 2007.Pirámide Documental, Gráfico 5.1. p 96.

13 *Ibíd*, p 38.

Declaración de aplicabilidad	Contiene los objetivos de control y controles contemplados en la norma ISO 27001 por el SGSI, basándose en el análisis de activos y recursos y la evaluación de riesgos, teniendo en cuenta la justificación tanto de inclusiones como de exclusiones de los controles.

Fuente: ALEXANDER, Alberto G. [14]

Procedimientos. Son documentos de nivel operativo. Presenta la planificación, operación y control de los procesos de la seguridad de la información. En general, son los procedimientos de gestión del sistema de seguridad de información. En este nivel de la documentación, es considerada una buena práctica tener todos los procedimientos exigidos por el manual, que están representados por medio de las cláusulas de obligatoria aplicación en la norma.

Instrucciones de trabajo. Se define como instrucción de trabajo a la "información que explica en detalle cómo se efectúa una operación concreta"[15]. Estos documentos describen cómo se realizan las actividades y tareas relacionadas con la seguridad de información. Usualmente contienen herramientas como listas de chequeo, flujo-gramas, tablas de decisión, formularios, anexos y ayudas visuales. La cuestión clave para identificar una instrucción de trabajo es si la ausencia de esta podría afectar negativamente la seguridad de la información.

Documentos. Este nivel agrupa los registros y los documentos del SGSI, y se evidencian en el cumplimiento de los requisitos y operación efectiva del SGSI. "… *se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI*"[16].

14 ISO 2700. Certificación, SGSI. En: El portal de ISO 27001 en español. [En línea]. [Consultado 9 de Mayo 2011] disponible en <http://www.iso27000.es/sgsi.html#section2c>

15 ALEXANDER, Alberto G. 2005. Diseño de un Sistema de Gestión de Seguridad de Información : Óptica ISO 27001:2005. Primera edición. Bogotá D.C. : Alfaomega Colombiana S.A., 2007. P 97.

16 INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Estándar Internacional ISO/IEC 27001 en español. [En línea]. Cláusula 4.3.3. [Consultado 2 de Mayo]. Disponible en <http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf>

3.2. ISO 27001:2005

La ISO 27001 hace parte de la serie 27000, es certificable y contiene los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI). En su Anexo A (Normativo), enumera resumidamente los objetivos de control y controles que desarrolla la ISO 27002:2005 de mejores prácticas (no certificable), para que las organizaciones los seleccionen en el desarrollo de sus SGSI. A pesar de que no es obligatoria la implementación de todos los controles, la empresa deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.[17]

Esta norma busca garantizar que la seguridad de la información sea gestionada correctamente, teniendo en cuenta un proceso sistemático, documentado y completamente conocido por todos los miembros de la empresa, basándose en un enfoque de riesgo empresarial.

3.2.1. Preliminar: Serie 27000

La ISO 27000 comprende una serie de estándares con un rango de numeración de comprende de la 27000 a 27019 y de la 27030 a 27044. Algunas de las normas están en procesos de desarrollo y no han sido oficialmente publicadas. La siguiente Tabla describe las normas ISO más significativas en el proceso de implementación de un SGSI para una organización.

Tabla 7. Serie 27000

ISO 27000	Contiene una introducción a los Sistemas de Gestión de Seguridad de Información, la descripción de la metodología del proceso mediante el ciclo PHVA y los términos con definiciones más importantes empleadas en los demás estándares.	Publicada en Mayo de 2009 y su contenido es público.	No certificable
ISO	Contiene los requisitos de un SGSI: las cláusulas de cumplimiento obligatorio, las cláusulas de apoyo y los anexos. En el anexo A se	Publicada en Octubre de 2005. En Colombia: NTC-	Certificable

17 ISO 27000. Certificación. En: El portal de ISO 27001 en español. [En línea]. [Consultado 19 de Mayo 2011] disponible en <http://www.iso27000.es/download/doc_iso27000_all.pdf>

27001	encuentran los controles que se deben seleccionar, el anexo B contiene los principios de la OECD y el modelo PHVA, y finalmente el anexo C indica la correspondencia entre las ISO 27001, 14001 y 9001.	ISO-IEC 27001.	
ISO 27002	Es la guía de buenas prácticas para la implementación del SGSI. Contiene una descripción más a fondo con recomendaciones de todos los objetivos de control y controles.	Publicada: Julio 2007. Colombia: NTC-ISO-IEC 27002.	No certificable
ISO 27003	Se origina por el anexo B de la 27001. Describe los pasos para el diseño del plan de implementación del SGSI.	Publicada en Febrero de 2010.	No certificable
ISO 27004	Es una guía para el uso de métricas para medir la eficacia del SGSI.	Publicada en Diciembre de 2009.	No certificable
ISO 27005	Establece el proceso para la gestión de los riesgos en la seguridad de información.	Publicada Junio/08. Colombia: NTC-ISO-IEC 27005.	No certificable

Fuente: Portal ISO 27000[18]

3.2.2. Proceso de implementación

El estándar de la ISO 27001 promueve la adopción de un modelo orientado al proceso, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI dentro de una organización.

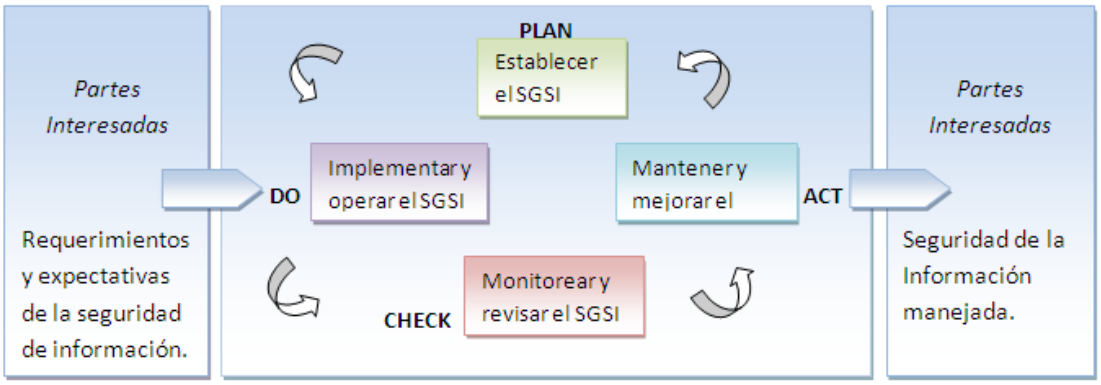
Este enfoque al proceso significa que hay unos recursos disponibles para la empresa, utilizados por ciertas actividades y manejados de forma que, teniendo en cuenta una serie de entradas (inputs), la transformación de estos insumos da origen a una serie de salidas (outputs), y que a la vez generalmente son la entrada directa (el input directo) de otro proceso.

Este estándar internacional se desarrolla en base al modelo PHVA (Planificar, Hacer, Verificar, Actuar), proporcionando solidez en la implementación de los principios de acuerdo a los lineamientos que presiden la evaluación del riesgo, el

18 ISO 2700. Certificación, SGSI. En: El portal de ISO 27001 en español. [En línea]. [Consultado 9 de Mayo 2011] disponible en < http://www.iso27000.es/iso27000.html#section3b>

diseño e implementación, gestión y monitoreo de la seguridad. Este modelo PHVA a su vez se puede aplicar a todos los procesos SGSI.

Figura 4. Modelo PHVA aplicado a los procesos SGSI



Fuente: INTERNATIONAL ORGANIZATION FOR STANDARIZATION[19]

Planificar. En esta etapa se establecen las políticas, objetivos, procesos y procedimientos del SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información, y entregar resultados en concordancia con las políticas y objetivos generales de la empresa[20]. Es muy importante la participación y aprobación de la Dirección en esta etapa.

En esta fase del ciclo se debe definir un alcance, una metodología, análisis y tratamiento de la evaluación de los riesgos, y la declaración de aplicabilidad (SOA: Statement Of Application). Podría decirse que al comenzar es la etapa de más duración, pues se inicia un proceso de conocimiento de la norma y sensibilización de la seguridad de información, además de que se deben impartir responsabilidades y crear un cronograma a seguir.

19 INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Estándar Internacional ISO/IEC 27001 en español. [En línea]. Cláusula 0.2. [Consultado 2 de Mayo]. Disponible en <http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf>

20 INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Estándar Internacional ISO/IEC 27001 en español. [En línea]. Primera edición 2005/10/15. p 7. [Consultado 2 de Mayo]. Disponible en <http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf>

Hacer. Consiste en implementar y operar la política, controles procesos y procedimientos del SGSI establecidos en la etapa de planeación[21]. Para lograrlo, se debe implantar el plan de tratamiento de riesgos, con el objetivo de implementar los controles seleccionados (que puedan llevar a cumplir con los objetivos de control) y poder monitorearlos, teniendo en cuenta la disponibilidad de recursos, la asignación de responsabilidades y el establecimiento de prioridades.

Es importante gestionar una formación y concienciación dentro de todo el personal de la organización, pues en la medida que todos los interesados participen activamente, se lograrán con mayos éxito y eficiencia los objetivos establecidos respecto a la seguridad de la información.

Verificar. Evaluar y medir el desempeño del proceso en comparación con la política donde es aplicable, objetivos y experiencias prácticas SGSI, y hacer reporte de los resultados para la revisión por parte de la gerencia[22].

El objetivo de esta fase es identificar incidentes de seguridad, detectar a tiempo errores que pasaron desapercibidos durante un proceso y prevenir amenazas. Las auditorías internas se deben realizar periódicamente, para revisar la efectividad del SGSI y de los controles; así como registrar acciones y tareas completadas y actualizar los planes de seguridad. Se pueden comunicar acciones de mejora para luego implementarlas en la etapa siguiente.

Actuar. Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI[23]. Tener en cuenta las lecciones aprendidas y comunicar las acciones realizadas.

---

21 *Ibíd*., p. 39
22 *Ibíd*., p. 39
23 *Ibíd.,* p. 39

3.2.3. Gestión de riesgos

La ISO 27001:2005 se basa en la gestión de riesgos para identificar las amenazas y vulnerabilidades de la empresa y seleccionar los controles que protegerán a los activos de información. Existen varias metodologías para gestionar los riesgos, cada organización puede llevar a cabo este proceso de la manera que mejor se ajuste a sus necesidades. Incluso algunas poseen su propia metodología de gestión de los riesgos estándar. Los riesgos deben ser identificados, analizados, evaluados y tratados.

Concepto de riesgo. Como se mencionó anteriormente, la gestión del riesgo es un proceso de suma importancia para la implementación de un SGSI. La ISO 27001:2005 señala una serie de pasos para llevar a cabo la evaluación de riesgos, lo cual comienza por la identificación de los activos de información, su tasación según los criterios de riesgo y el cálculo de éste. Seguidamente, se debe establecer el tratamiento que se dará a los riesgos, si será aceptarlo, evitarlo o transferirlo. Por último, se seleccionan los controles del Anexo A del estándar según el análisis de riesgo realizado y se implantan dichos controles, sin dejar de lado el riesgo residual[24].

Un riesgo se define como la "*posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información*", Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias[25]. Por lo tanto un riesgo es la consecuencia del desconocimiento o inapropiada gestión de amenazas y vulnerabilidades; y existen varias metodologías para el análisis del riesgo, que generalmente se utiliza la establecida por la organización.

---

24 Riesgo residual: El riesgo remanente luego de una amenaza a la seguridad. Disponible en <http://www.iso27000.es/download/analisis_ISO-27001.pdf>

25 ISO 2700. Certificación, SGSI. En: El portal de ISO 27001 en español, Glosario. [En línea]. [Consultado 9 de Mayo 2011] disponible en < http://www.iso27000.es/glosario.html#section10r>

Amenazas y vulnerabilidades. Las amenazas son factores que pueden generar un incidente y tener consecuencias graves a la organización. Según Alberto G. Alexander, una amenaza es "*una indicación de un evento desagradable con el potencial de causar daño*"[26]. Las vulnerabilidades por otro lado, tienen que ver con las debilidades de la empresa respecto a su seguridad en los activos. Pueden verse como una 'puerta' abierta para que una amenaza 'entre' y perjudique la información.

Entre las vulnerabilidades, el autor anteriormente mencionado clasifica las vulnerabilidades por control de acceso, seguridad de los recursos humanos, seguridad física y ambiental, gestión de operaciones y comunicación y mantenimiento, desarrollo y adquisición de sistemas de información. Algunos ejemplos son: falta de entrenamiento en seguridad, gestión de red inadecuada, contraseñas débiles, etc.[27]

3.2.4. Estructura y cláusulas

La norma ISO 27001:2005 como tal, contiene un prefacio, introducción, definición y representación del alcance del modelo, las referencias normativas, términos y definiciones claves, el SGSI y los anexos A, B y C. El anexo A (normativo) contiene una tabla detallada de los objetivos de control y controles, agrupados por medio de conceptos concernientes a la seguridad de la información. El estándar recomienda el seguimiento de la guía de buenas prácticas ISO 27002:2005, anterior ISO 17799:2005. La Tabla 8 muestra el contenido de la norma.

26 ALEXANDER, Alberto G. Diseño de un Sistema de Gestión de Seguridad de Información : Óptica ISO 27001:2005. Primera edición. Bogotá D.C. : Alfaomega Colombiana S.A., 2007. P 48.
27 *Ibíd.,* p. 39

Tabla 8. Contenido de la ISO 27001:2005

Cláusula 0	Introducción. Generalidades e introducción al método PHVA.
Cláusula 1	Objeto y campo de aplicación. Se especifica el objetivo, la aplicación y el tratamiento de exclusiones.
Cláusula 2	Referencias normativas. Otras normas que sirven de referencia.
Cláusula 3	Términos y definiciones. Breve descripción de términos más usados.
Cláusula 4	Sistema de gestión de la seguridad de la información. Cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI; requisitos de documentación y control de la misma. De obligatorio cumplimiento.
Cláusula 5	Responsabilidad de la dirección. En cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal. Cláusula de obligatorio cumplimiento.
Cláusula 6	Auditorías internas del SGSI. Cómo realizar las auditorías internas de control y cumplimiento. Cláusula de obligatorio cumplimiento.
Cláusula 7	Revisión del SGSI por la dirección. Cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección. Cláusula de obligatorio cumplimiento.
Cláusula 8	Mejora del SGSI. Mejora continua, acciones correctivas y acciones preventivas. Cláusula de obligatorio cumplimiento.
Anexo A	Objetivos de control y controles. Anexo normativo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 27002:2005.
Anexo B	Relación con los Principios de la OCDE. Anexo informativo con la correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE.
Anexo C	Correspondencia con otras normas. Anexo informativo con una tabla de correspondencia de cláusulas con ISO 9001 e ISO 14001.
Bibliografía	Normas y publicaciones de referencia.

Fuente: Portal ISO 27000[28]

28 ISO 27000. Certificación. En: El portal de ISO 27001 en español. [En línea]. [Consultado 19 de Mayo 2011] disponible en <http://www.iso27000.es/download/doc_iso27000_all.pdf>

4. PLAN DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN BASE A LA ISO 27001:2005

El plan de ejecución (o plan de implementación, como se llamará en adelante en este documento) de un Sistema de Gestión de Seguridad de Información basado en la norma ISO 27001:2005, para su aplicación en la Fundación Cardiovascular de Colombia, se ha tomado como un gran proyecto para la Dirección de Tecnología Informática, pues al ser los gestores principales de la información en la empresa, busca ser el pionero de la gestión de seguridad de información tanto en el área como en toda la organización.

Este plan de implementación se ha creado con el fin de establecer una base para el proceso de implementación del SGSI en la Dirección de Tecnología Informática, de manera que adquirir la certificación por medio del ICONTEC sea una meta clara y definida, y se materialice a través de las actividades realizadas. Como guía para su elaboración se utilizó la ISO 27001:2005 y un soporte de la Metodología de implantación y certificación de ISO27001[29], pero también se tuvo en cuenta la experiencia adquirida en la FCV.

Se definirán los objetivos, la justificación, la metodología elaborada, las responsabilidades y el proceso el cual consta de seis fases. En la sección 4.5 se define cómo orientar el proceso en base al estado actual. La metodología para la gestión del riesgo se describe en el numeral 4.6.

Los pasos para establecer el SGSI al interior de la empresa se encuentran en la sección 4.7, y la 4.8 se define cómo implementarlo. Finalmente, las secciones 4.9 y 4.10 describen el proceso de control y mejora respectivamente.

29 CORLETTI, Alejandro (Ph.D. Ingeniería Informática. Director de Seguridad Informática NCS Consultoría Tecnológica, España 2008). La Flecha. En: Seguridad, Artículos. [En línea]. [Consultado 17 Junio 2011]. Disponible en <http://www.laflecha.net/canales/seguridad/articulos/metodologia-de-implantacion-y-certificacion-de-iso27001>

4.1. OBJETIVOS DEL PLAN DE IMPLEMENTACIÓN

El principal objetivo del plan de implementación es construir un camino, una base para la implantación de un Sistema de Gestión de Seguridad de Información en la empresa; de manera que cuando sea aprobado el proyecto (presupuesto y plan de acción 2012) para la certificación con la ISO 27001:2005, exista una guía y el proceso no se lleve a cabo bajo ningún fundamento.

4.1.1. Objetivos específicos

- Establecer las pautas para implantar un SGSI con todos sus requerimientos en base a la normativa y requisitos de la ISO 27001:2005 para la Dirección de Tecnología Informática.

- Desarrollar y llevar a cabo el plan de implementación de un SGSI en la Dirección de Tecnología Informática de la Fundación Cardiovascular de Colombia por medio de la experiencia vivida en la práctica.

- Crear una metodología para la gestión y tratamiento de los riesgos para la posterior selección de controles y protección de los activos de información.

4.2. JUSTIFICACIÓN

La implementación de un Sistema de Gestión de Seguridad de Información requiere de una gran inversión de tiempo, recurso humano y dinero. Si una organización planea gestionar su seguridad de información por medio de un SGSI en base a la ISO 27001, la creación de un plan de implementación puede definir el éxito del proceso.

¿Cómo? En este tipo de proyectos para sistemas de gestión, la planificación es un elemento clave, pues al tener conocimiento de lo que se va a hacer, cómo, con quién, cuándo y con cuánto, es posible medir la eficacia y eficiencia del proceso, identificar los errores que impiden el cumplimiento de los objetivos y establecer acciones de mejora.

Aunque es posible guiar el proceso de implementación por medio de consultores u otro tipo de ayuda externa, de esta forma es más costoso y probablemente la empresa no estaría al tanto de todos los detalles del proceso, y es sumamente importante tener conocimiento de los avances, requisitos e inconvenientes que se puedan presentar, pues es de esta manera que se aprende de los errores.

4.3. RESPONSABILIDADES

Líder del proyecto de seguridad de información: esta persona estará encargada de gestionar el proceso, proporcionar las directrices, asignar las tareas principales, crear el cronograma, comunicar al equipo, aprobar los procedimientos y documentos creados, tomar decisiones, presentar las propuestas a la Dirección y convocar al Comité de Seguridad de Información.

Ingeniero Monitor: encargada de hacer el seguimiento del proceso, las tareas y documentos elaborados por el analista. Sus labores se orientan a la calidad de los procesos; debe revisar la documentación creada y convocar las reuniones con el equipo de seguridad de información.

Analista de seguridad: labor llevada a cabo por la autora de este proyecto, y practicante de la FCV. Persona encargada de completar las actividades establecidas en el cronograma y realizar las tareas necesarias para cumplir con los requisitos identificados.

Comité de Seguridad de Información: su responsabilidad es establecer las directrices y dar la aprobación final de los resultados de las actividades realizadas. Deben tomar las decisiones importantes que pueden generar gran cambio en el proceso, por ejemplo aquellas que se relacionan con presupuesto y políticas a nivel organizacional.

4.4. METODOLOGÍA DE IMPLANTACIÓN

La metodología se elabora en base al estándar internacional ISO 27001:2005 – SGSI y al ciclo PHVA, el conocimiento adquirido en la FCV respecto a sistemas de gestión, investigación sobre seguridad de información y otras fuentes bibliográficas y normativas. La experiencia laboral adquirida en la práctica empresarial permitió el desarrollo de este plan de implementación, pues la empresa y la Dirección de Tecnología Informática dispusieron de los recursos para ahondar el conocimiento del tema y concluir el proyecto.

Tabla 9. Etapas metodología proceso de implementación

Etapa	Sub Etapa	Fase	Descripción	Responsable
Planificar	Planificar	1	Definición de responsabilidades, elaboración del cronograma, seguimiento (reuniones), recursos, tiempos.	Líder, Ingeniero Monitor
	Gestionar	1	Obtener la aprobación de la Dirección y tener en cuenta los objetivos estratégicos. Determinar el estado en el que se encuentra la DTI respecto a la seguridad de información	Líder, Ingeniero Monitor
	Evaluar	2	Valorar y calcular los riesgos	Analista de Seguridad
	Analizar	2	Identificar los riesgos más importantes y analizar los riesgos.	Líder, Ingeniero Monitor, Analista de Seguridad
Hacer	Divulgación	3	Estructurar los procedimientos de gestión del SGSI y sensibilizar al personal.	Analista de Seguridad

	Implementar	4	Impartir planes de formación y concientización, crear documentación soporte a los controles. Implantar políticas.	Analista de Seguridad
Verificar	Control	5	Detectar los errores en los resultados de la gestión de riesgos. Identificar eventos de seguridad.	Analista de Seguridad, Ingeniero Monitor
	Revisión	5	Realizar auditorías internas del SGSI. Revisiones por parte de la Dirección.	Auditor responsable, Dirección
Actuar	Seguimiento	6	Asegurar la continuidad de las actividades, apoyar al personal en el proceso.	Analista de Seguridad, Ingeniero Monitor
	Mejora	6	Implementar acciones de mejora.	Líder, Ingeniero Monitor, Analista de Seguridad

Fuente: Autora

4.5. FASE 1: ANÁLISIS DE LA SITUACIÓN ACTUAL

En esta fase se pretende definir en qué punto está la UEN, Dirección o Área implicada respecto a los requisitos de la ISO 27001:2005. Se describirán las actividades que corresponden tanto a las exigencias de la norma como a las tareas que soportan la completitud de los requerimientos.

4.5.1. Identificar información relevante

Es el primer paso a seguir, ¿qué se debe proteger?, ¿qué es importante y qué no?, ¿cuál es la información relevante?

Para identificar dicha información, se debe comenzar por los procesos de la línea base de la empresa. Se elaboró el formato de la Matriz de Flujo de Información (Ver Anexo 1) para identificar la información de entrada y salida entre los procesos. Para completar la matriz se debe tener en cuenta:

- El nombre del proceso
- La actividad del proceso (deben mencionarse todas las actividades relevantes propias del área). Si es un Área o UEN muy grande, se pueden subdividir las actividades.
- La información generada en cada actividad. Aunque se debe tener en cuenta la información de entrada, la que realmente interesa es la de salida.
- El responsable de la realización de la actividad y por tanto de la información de salida.
- El código de la caracterización del proceso y fecha de aprobación por el Departamento de Planeación y Calidad.

Este documento permite recopilar la información que se maneja, sabiendo quién lo hace y qué tan actualizado está el registro que se tiene sobre ella.

ENTREGABLE: Matriz de flujo de información

4.5.2. Definir el alcance del sistema

En el alcance se documentan los procesos que el Sistema de Gestión de Seguridad de Información abarcará; así como los procesos excluidos y la justificación de dicha decisión. El alcance del SGSI es muy importante, ya que esto definirá el Área, Dirección o UEN de cuyos activos de información se protegerán, qué medidas se tomarán, los procesos de negocio involucrados, quién dirige el proceso de implementación y las necesidades de seguridad.

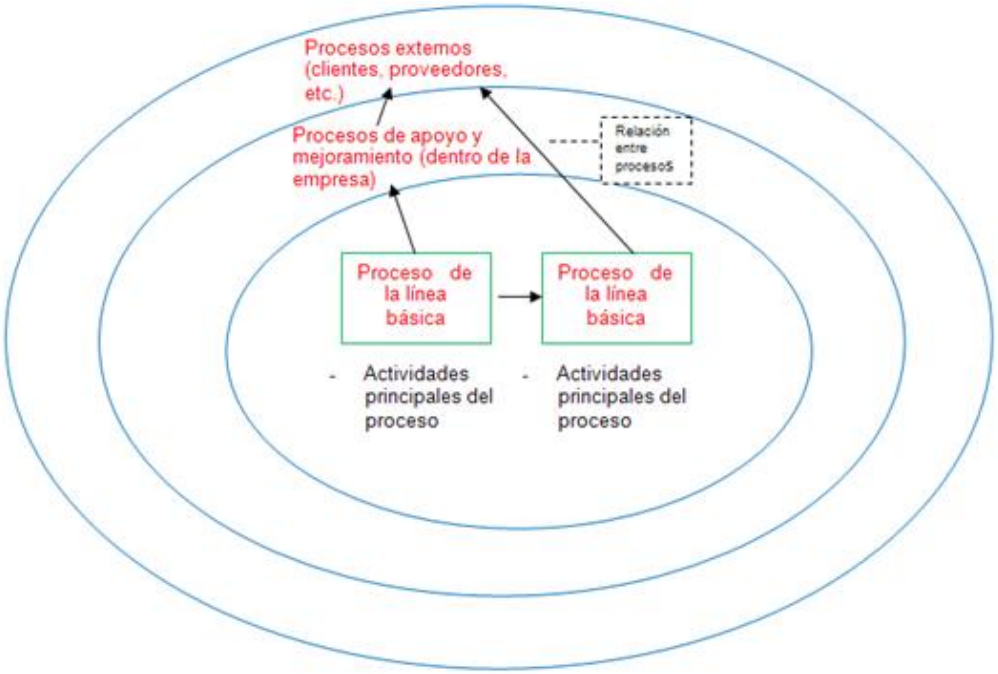
Es recomendable definir inicialmente un alcance reducido que permita un seguimiento controlable y no lleve al fracaso inmediato, además que dé paso al aprendizaje. En el momento de redactar el documento de alcance, se deben tener en cuenta los siguientes aspectos:

Compromiso institucional. La Dirección expone su compromiso frente al proceso y el apoyo brindado. Se deben definir los objetivos y el perfil de la empresa (Área, Dirección o UEN).

Límites del SGSI. Se definen las especificaciones del alcance. Los procesos implicados, terceros y externos y los procesos excluidos; además se deben incluir las localizaciones y los sistemas de información, estos con el fin de clarificar qué partes de la organización se certificarán, que son aspectos de gran importancia en el momento de una auditoría.

Interfaces del SGSI. Representación gráfica de la interacción entre los procesos. El diagrama de las elipses es de gran ayuda para visualizar este aspecto, y además permite identificar los activos de información. Ver Figura 5.

Figura 5. Diagrama de elipses de la interacción entre procesos



Fuente: Autora

Marco legal. Se debe definir el marco legal vigente aplicable a los procesos del alcance.

ENTREGABLE: Documento del alcance del Sistema de Gestión de Seguridad de Información.

4.5.3. Identificación de los activos de información

Como requisito del estándar, se deben listar los activos de información. El inventario o registro de activos de información (como se llamará en este plan de implementación ya que el registro implica que es más completo que un inventario), permitirá visualizar los más importantes de la UEN, Dirección o Área implicada; los responsables por su uso, su ubicación, cómo se almacena la información y su prioridad. De manera que se cuenta con un inventario organizado de las propiedades más importantes de la FCV.

Teniendo ya la información relevante, se pueden listar los activos de información en base a unos lineamientos de clasificación. El registro debe indicar el nombre del activo de información, una breve descripción, el responsable y las directrices para la clasificación como se especifica en la Tabla 10.

Tabla 10. Lineamientos de clasificación para activos de información

Criterio de clasificación		**Especificación**	**Ejemplo**
DISTRIBUCIÓN **(forma en que se comparten los activos de información en la empresa)**	Interna	Sólo permitido dentro de la organización	Cartas, memos, contratos internos
	Externa	Por fuera de la empresa	Contratos con externos
	Electrónica	Información en tránsito, puede requerir encriptación de datos	Correo interno
	Correo físico	Protocolos de envío	Correo externo a otras ciudades

MEDIO/LUGAR DE ALMACENAMIENTO **(dónde o cómo se almacenan los activos de información)**	Digital	Información digital	Medios magnéticos, ópticos, CD, DVD, discos duros, etc.
	Repositorios	Datos o información almacenada	Bases de datos o información en línea de la compañía o en servidores
	Físico	Tiene una ubicación física en las localizaciones de la empresa	Documentos impresos, correo físico
	Lugar	En el caso de activos de información físicos, dónde se encuentran	Oficinas, bodegas
TIPO **(clasificación general de los activos de información)**	Información	Toda información y/o datos digitales	e-mail, planillas, documentos y archivos digitales. Datos, manuales de usuario, etc.
	Documentos físicos	Información en papel	Documentos impresos, contratos, acuerdos de confidencialidad, memorándum, registros, entre otros.
	Software	Sistemas operativos, aplicaciones y herramientas software (propias o de terceros), sistemas ERP, CRM, Business Intelligence, entre otros.	--
	Físicos	Infraestructura, ambientes físicos, cableado estructurado, antenas, hardware, computadoras, medios magnéticos, entre otros.	Datacenter, oficinas, salas de recepción, cámaras de seguridad, etc.
	Recurso humano	Colaboradores, funcionarios, clientes, terceros. Generalmente se indica al personal como un activo de información, usando el nombre del cargo o la función.	Gerentes, directores, jefes, coordinadores, secretarias, practicantes, analistas, administradores, ingenieros, auxiliares, etc.
	Servicios	Servicios prestados por la UEN, Dirección o Área, así como los brindados por terceros	Mantenimiento, servicios salud
	Intangibles	Conocimiento, ventaja competitiva, imagen corporativa, credibilidad y percepción de la empresa, reconocimiento	--
	Legislativos	Obligaciones legales y contractuales	--

CATEGORÍA **(según administración, control y nivel de las propiedades de información)**	Pública sin clasificar	Información no confidencial, puede ser pública sin implicaciones para la FCV. La pérdida de disponibilidad no supone un alto impacto. La integridad es importante pero no vital.	*Brochures*, Información de dominio público, Versiones de prueba de SW, Reportes financieros requeridos por autoridades reguladoras, Boletines de noticias para transmisión externa
	Privada	Información restringida de acceso interno. La falta de confidencialidad puede comprometer las actividades, causar pérdidas financieras, dar ventaja a competidores o provocar descenso en la confianza del cliente. Integridad de la información es vital.	Contraseñas e información de procesos de seguridad de la compañía. *Know how* para procesar la información del cliente. Procesos operacionales usados en todas las UEN. Todo código desarrollado de la compañía.
	Datos confidenciales clientes	Información de clientes en cualquier forma para su procesamiento. Copia original no debe ser cambiada de ninguna forma sin permiso del cliente. Altos niveles de integridad, confidencialidad y disponibilidad requeridos	Información del producto generado para el cliente, Bases de datos IPS (Instituciones Prestadoras de Servicios), Historia clínica, Datos personales (pacientes, clientes)
	Datos confidenciales compañía	Información procesada y usada por la compañía en relación a sus procesos de negocio. Acceso muy restringido internamente. Máximo nivel de integridad, confidencialidad y disponibilidad requerido.	Salarios y otros datos del personal. Datos de contabilidad y demás reportes financieros. Datos confidenciales y contratos confidenciales. Planes de negocio. Acuerdos de no divulgación.

Fuente: Autora

ENTREGABLE: Registro de los activos de información. (Ver Anexo 2).

4.5.4. Análisis de brecha

Análisis de brecha o Gap Analysis, permite revisar los controles que están actualmente implementados y en qué nivel, analizando la situación actual de la empresa para identificar cómo se debe actuar en el proceso y qué falta por hacer.

En base a una lista de chequeo (Ver Anexo 3) y al análisis que se realice se puede evidenciar en qué punto está la empresa respecto a los requerimientos de la ISO 27001:2005. Por otro lado, se deben presentar recomendaciones y observaciones

para el desarrollo de aquellos controles que tienen un nivel de implementación que necesita ser mejorado, documentado o monitoreado.

Este documento tiene como fin clarificar y advertir la brecha existente entre los controles actualmente implementados en la empresa, contrastados con la calidad y nivel de los controles que debieran estar implantados para obtener la certificación. También se busca encaminar el proceso que se debe seguir para implementar los controles que faltan, y aquellos que requieren mayor nivel de implementación y definir los que no aplican. El proceso será más eficiente, ya que teniendo en cuenta la situación actual, se evitan redundancias, inconsistencias y trabajo extra.

¿Cómo elaborarla? Se tomó como base el formato de la Declaración de Aplicabilidad (Ver Anexo 4). Para definir la aplicabilidad actual de cada control, se deben seguir el instructivo del Anexo 7.

ENTREGABLE: Análisis de brecha de los controles.

4.6. FASE 2: ANÁLISIS Y GESTIÓN DE RIESGOS - METODOLOGÍA

En esta fase se busca definir el enfoque de la gestión de los riesgos, identificar las amenazas que pueden generar daños y las vulnerabilidades de la empresa. Se divide en dos etapas principales: la definición del enfoque de gestión del riesgo y el análisis y evaluación de los riesgos. Todo esto anterior se resume a una metodología de riesgo elaborada por la autora, adaptada a las necesidades de la FCV.

La gestión del riesgo implica que se deben **identificar** los factores que lo producen, **analizar** el impacto que pueden llegar a tener en la empresa, **valorar**

los niveles de riesgo, **evaluar** su peligrosidad y buscar opciones para **tratar** los riesgos que más exponen a los activos de información.

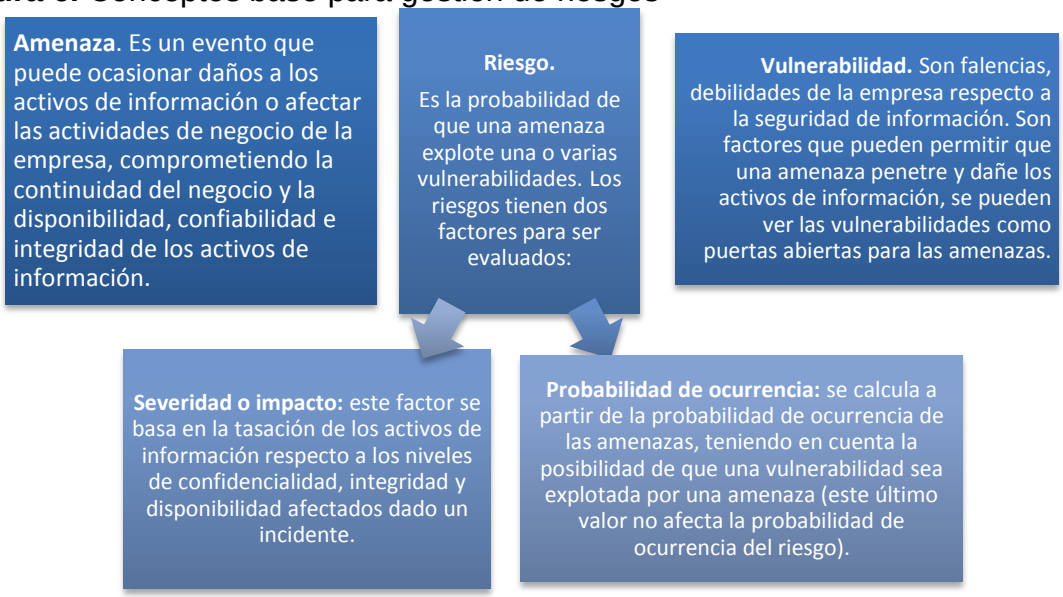
ENTREGABLES:

- Matriz de relación amenazas y vulnerabilidades.
- Mapa de riesgos.
- Informe medición de riesgos.

4.6.1. Introducción a la metodología de gestión de riesgo

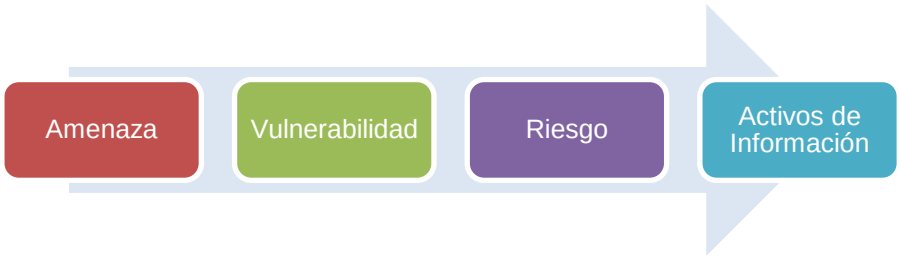
En este capítulo se describe la metodología a seguir para gestionar los riesgos de conformidad a los requisitos, conceptos y recomendaciones de la ISO 27001:2005. A pesar de que se realizó un proceso de estandarización de una metodología de gestión de riesgos en la FCV (elaborada en el Departamento de Planeación y Calidad) orientada a los riesgos sobre procesos y riesgos estratégicos; ésta se debió ajustar a la norma, ya que se requiere un análisis de riesgos enfocado a los activos de información. A medida que se desarrolla la metodología se presentará la relación entre los conceptos base.

Figura 6. Conceptos base para gestión de riesgos



Fuente: ISO27001. Autora

Figura 7. Relación causa-probabilidad-efecto entre componentes de la gestión de riesgos



Fuente: ALEXANDER, Alberto G. Cálculo de las amenazas y vulnerabilidades[30]

4.6.1.1. Objetivos gestión de riesgo

- El objetivo principal de esta metodología para la gestión de riesgos es establecer una base para el análisis y evaluación de riesgos, teniendo en cuenta los requerimientos y cláusulas de la ISO 27001:2005.

[30] ALEXANDER, Alberto G. Diseño de un Sistema de Gestión de Seguridad de Información : Óptica ISO 27001:2005. Primera edición. Bogotá D.C. : Alfaomega Colombiana S.A., 2007. p 52.

- Plantear los pasos a seguir para el análisis y gestión de riesgos, de manera que se pueda aplicar a futuro para un alcance más amplio del SGSI en la empresa.

- Definir las pautas para los niveles, tratamiento y documentación de los riesgos a los activos de información.

4.6.2. Identificación de amenazas y vulnerabilidades

Para identificar las amenazas y vulnerabilidades, se tienen en cuenta distintos elementos de las posibles causas de riesgo y la clasificación por las posibles áreas de negocio afectadas. También se acude a la información ya existente sobre las amenazas que pueden afectar a los activos de información, teniendo en cuenta en este caso la tabla de amenazas y vulnerabilidades de la ISO 27005:2008 para la Gestión de Riesgo en la Seguridad de Información, el mapa de riesgos informáticos del Departamento de Tecnología Informática y otras consultas bibliográficas[31]. Es recomendable elaborar una matriz de amenazas y vulnerabilidades donde se relacionen y distinga cada una de ellas, previo a calcular su probabilidad de ocurrencia (Ver Anexo 6).

El proceso de identificación de riesgos debiera ser continuo, considerando otras formas de identificar amenazas y vulnerabilidades tales como *brain-storming* (lluvia de ideas), entrevistas con los responsables de los activos de información, diagramas de flujo, análisis de incidentes previos, entre otros. Esta clasificación se basó en la lista de amenazas de la ISO 27005 y otras ya identificadas por la Dirección de Tecnología Informática de la FCV.

[31] ALEXANDER, Alberto G. Diseño de un Sistema de Gestión de Seguridad de Información : Óptica ISO 27001:2005. Primera edición. Bogotá D.C. : Alfaomega Colombiana S.A., 2007. p 48-51.

Es importante evaluar cada activo de información con toda amenaza identificada aún cuando ésta no aplique, de esta manera se asegura que el responsable del activo de información pueda llevar a cabo la tasación contando con todas las posibilidades y tipos de amenazas.

Clasificación. La clasificación de amenazas y vulnerabilidades se lleva a cabo teniendo en cuenta las categorías que se ajustan más a los activos de información y procesos de la empresa, de forma que sean fácilmente asimiladas y haya claridad en los tipos de incidencias. Las categorías se asignaron de la siguiente manera:

Tabla 11. Clasificación amenazas

Amenazas			
Categorías por tipo		Clasificación por origen	
Legales	Implica acciones legales	**Accidental**	Amenazas que se originan por errores o actuaciones no intencionales por parte del personal de la organización.
Social	Acciones personas externas		
Tecnologías informáticas	Infraestructura, software, redes	**Deliberado**	Acciones intencionales, premeditadas o que se llevan a cabo con el fin de dañar los activos de información.
Eventos naturales	Desastres naturales		
Física	Instalaciones	**Ambiental**	Eventos -accidentales- que no tienen que ver con acciones humanas, incidentes causados por desastres naturales.
Operacional	Procesos propios de la empresa		
Recurso Humano	Acciones del personal		

Fuente: ISO 27005[32]. Autora

32 Archivo digital en los servidores de la Fundación Cardiovascular de Colombia.

Tabla 12. Clasificación vulnerabilidades

Vulnerabilidades
Recursos humanos
Redes y telecomunicaciones
Infraestructura
Control de acceso, información y bases de datos
Instalaciones físicas
Software, sistemas de información y desarrollo
Gestión operativa y organizacional (gestión estratégica, asuntos legales, procedimientos y políticas corporativas, etc.)

Fuente: ISO 27005[33]. Autora

Relación amenaza – vulnerabilidad. Para poder deducir la posibilidad de que una amenaza explote una vulnerabilidad y calcular la probabilidad de ocurrencia de una amenaza, es necesario relacionarlas de acuerdo a una evaluación de las potenciales causas para que una amenaza se dé. Esta relación se presenta en la matriz de amenazas y vulnerabilidades que se ha recomendado elaborar.

Entrevista con propietarios de activos de información. Dado que los propietarios de los activos de información son los responsables por el mismo (definen acciones permitidas, derechos de acceso, correcto uso y/o implementación, documentación, seguridad, control y seguimiento), deben ser ellos mismos quienes evalúen los niveles de confidencialidad, integridad y disponibilidad de los activos de información comprometidos ante un evento de seguridad; lo cual determina el impacto al negocio dada una incidencia. Igualmente deben definir la probabilidad de ocurrencia de una amenaza.

33 *Ibíd*, p 59.

Para esto se recomienda realizar una entrevista con los jefes ó líderes del área responsable del activo de información, junto con aquellos involucrados directamente con éste. De manera que la decisión de los niveles, probabilidades e impacto de riesgos están en manos del líder; fundamentada en las consideraciones brindadas por el personal con responsabilidades directas sobre el activo de información.

Con esto se busca tener una única persona quien tome las decisiones respecto al trato de los activos de información, teniendo en cuenta el compromiso en igual medida de personal involucrado con el activo. Estas decisiones son subjetivas a cargo del responsable del activo de información.

Tasación de activos de información. Este paso pretende evaluar los activos de información basándose en cómo se ven comprometidos dado un evento de seguridad, para así identificar y determinar cuáles son los más críticos y al mismo tiempo definir el impacto que causaría en el negocio la pérdida de integridad, confidencialidad y disponibilidad sobre los activos de información. De esta manera en el Mapa de Riesgos se pueden calcular los niveles de riesgo y seleccionar las opciones tratamiento adecuado para cada activo de información.

Teniendo la lista de activos de información (identificados en el inventario y registro de activos de información en la primera fase) con sus respectivos propietarios o responsables, se debe evaluar cada uno de ellos por su criticidad frente a los niveles de disponibilidad, confidencialidad e integridad. Se deben tasar los activos de información cuestionando cómo -en qué nivel- un incidente afectaría los niveles de dichas propiedades, en base a la siguiente escala de valores y respondiendo a:

¿Cómo afecta al activo de información la falta de disponibilidad, integridad o confidencialidad? 1: Muy poco, 2: Poco, 3: Moderado, 4: Alto.

En el Mapa de Riesgos se encuentra la hoja de cálculo correspondiente a la tasación de activos de información. El total corresponde al promedio aritmético de los valores en los niveles de las propiedades de los activos de información.

4.6.3. Análisis de riesgo

El análisis de riesgos se realizar a partir del proceso de identificación anteriormente enunciado, e implica calcular las probabilidades de ocurrencia y determinar el impacto que tendría en la empresa un incidente que pueda perjudicar a los activos de información.

Factores de riesgo. Como bien se mencionó anteriormente, los factores de riesgo son el impacto y la probabilidad de ocurrencia. Estos valores son los que se deben tener en cuenta para el Mapa de Riesgos.

Los valores de la Tabla 13 se utilizan para la valoración de la probabilidad de ocurrencia de las amenazas. Y en la Tabla 10 se establecen los criterios del impacto del negocio en base al resultado total de la tasación de activos de información.

Tabla 13. Valor de los factores de riesgo por criterio: probabilidad de ocurrencia

PROBABILIDAD DE OCURRENCIA (P) - Amenazas	
Criterio	**Valor**
ALTA (76-100%): Es muy probable que ocurra la amenaza	4
MEDIA (51-75%): Es probable que ocurra a corto plazo	3
BAJA (26-50%): Es posible que suceda	2
MUY BAJA (0-25%): Es improbable que la amenaza ocurra	1

Fuente: Autora

Tabla 14. Valor de los factores de riesgo por criterio: impacto

IMPACTO DEL NEGOCIO (I) - Activos de información	
Criterio	**Valor**
ALTO: Puede causar pérdidas o daños severos (irremediables) de costos muy altos	4
MEDIO: Puede causar daños costosos	3
BAJO: Puede ocasionar pequeñas pérdidas con costo	2
MUY BAJO: Puede causar pequeños daños de costo insignificante	1

Fuente: Autora

Nivel de riesgo. Los niveles de riesgo y criticidad se definieron por medio de reuniones con ingenieros de calidad, teniendo en cuenta que es importante definir criterios que permitan eficiencia en el proceso de análisis de riesgo, orientado a un proceso sencillo e intuitivo. Se tiene en cuenta el criterio de aceptación del riesgo de acuerdo al nivel de criticidad.

Tabla 15. Nivel de criticidad del riesgo (criterios para la aceptación)

ALTO	Riesgo significativo, inaceptable; requiere atención inmediata y una investigación detallada.
MEDIO	Moderado, requiere atención especial por parte de la Gerencia y especificación de responsabilidades para mitigarlo.
BAJO	Riesgo insignificante y aceptable. Debe ser mitigado por procedimientos rutinarios de la empresa.

Fuente: Autora

El nivel de riesgo corresponde al producto de la probabilidad de ocurrencia y el impacto al negocio, teniendo en cuenta los niveles de criticidad del riesgo.

Tabla 16. Niveles de riesgo

Probabilidad de Ocurrencia	Impacto del Negocio			
	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

Fuente: Autora

Cálculo de amenazas y vulnerabilidades. El cálculo de la probabilidad de ocurrencia de una amenaza se relaciona directamente con la probabilidad de ocurrencia del nivel de riesgo. Esta probabilidad se basa en la posibilidad que existe de que una vulnerabilidad sea explotada por una amenaza, pero éste valor no se tiene en cuenta para el valor utilizado en el cálculo del nivel de riesgo (dado que por cada amenaza hay más de una vulnerabilidad relacionada).

Para definir tanto la probabilidad de ocurrencia de la amenaza como la posibilidad de la vulnerabilidad (de ser explotada), se deben tener en cuenta los valores sobre los criterios de los factores de riesgo. Pero se utilizará solamente el valor de las amenazas para calcular el nivel de riesgo (el factor probabilidad de ocurrencia)

4.6.4. Evaluación del riesgo

En esta etapa se calcula el nivel de riesgo y se realiza la matriz de riesgos. Esta fue elaborada teniendo como base la Matriz para el Análisis de Riesgo[34]. Se crearon distintos modelos para el mapa de riesgos, pero el presentado en este documento fue el resultado de un arduo análisis y adaptación para los activos de información.

34 ERB, Markus. Gestión de Riesgo en la Seguridad Informática [Blog]. Matriz para el análisis de riesgo. [En línea]. [Consultado 22 de Julio 2011]. Disponible en <http://protejete.wordpress.com/gdr_principal/matriz_riesgo/>

4.6.4.1. Cálculo del riesgo

Se debe calcular la posibilidad de que una vulnerabilidad sea explotada por una amenaza y cause un riesgo. Por lo tanto es necesario establecer una probabilidad de ocurrencia para las amenazas basándose en la posibilidad de explotación de vulnerabilidad. De esta manera se puede realizar el análisis de riesgos (la probabilidad de ocurrencia de un riesgo equivale a el cálculo de la posibilidad de que una amenaza ocurra y aproveche una vulnerabilidad, y den paso a un incidente).

Riesgo = **Probabilidad Ocurrencia** (amenazas) * **Impacto al negocio** (sobre los activos de información)

Probabilidad Ocurrencia = (cálculo de la probabilidad de que ocurra una amenaza determinada, teniendo en cuenta las posibilidades de explotación de las vulnerabilidades para cada amenaza)

Impacto = (total del valor de los niveles de confidencialidad, integridad y disponibilidad de la tasación de activos)

NOTA: La probabilidad de ocurrencia de una amenaza se calcula en base a la posibilidad de que una vulnerabilidad sea explotada, pero ésta posibilidad de la vulnerabilidad no afecta al valor de la probabilidad de ocurrencia del riesgo.

4.6.4.2. Mapa de riesgos

En la matriz de riesgos se relacionan todos los valores y cálculos realizados anteriormente. A medida que se realiza la tasación de activos y el cálculo amenaza-vulnerabilidad, el Mapa de Riesgos se debe completar dando a conocer

los niveles de riesgo, los niveles de prioridad de los activos de información y el grado de peligrosidad de las amenazas.

En el mapa de riesgos elaborado para la DTI (Ver Anexo 17) no se evalúa una probabilidad de ocurrencia para cada activo de información, pues esto implicaría elaborar una matriz de riesgos demasiado grande y costosa (cada activo de información se evaluaría por cada amenaza con su propia probabilidad), y por lo tanto ineficiente (ya que no está orientada a procesos). Se tiene entonces una sola probabilidad de ocurrencia para cada amenaza, que se debe determinar de acuerdo al activo de información más afectado. Esto dará paso a errores en los cálculos del nivel de riesgo, pero será más eficiente y menos costoso que elaborar una matriz de tres dimensiones.

El nivel de prioridad corresponde al promedio aritmético de las filas del mapa de riesgos, permite valorar los activos de información de acuerdo al nivel en el que las amenazas lo afectan, por la probabilidad de ocurrencia y por su impacto al negocio. Los valores de los rangos se pueden ver en la Tabla 17.

Tabla 17. Nivel de prioridad del activo de información

Promedio filas PxI - (pPI)	Prioridad
pPI <= 4	Baja
4 < pPI <= 9	Media
9 < pPI <=16	Alta

Fuente: Autora

El grado de peligrosidad de la amenaza se mide en base al grado de exposición al riesgo. Se obtiene por el producto de tres factores:

Grado de Peligrosidad (GP) = Probabilidad Ocurrencia (P) x Impacto (I) x Exposición (E)[35]

La exposición del riesgo corresponde a la frecuencia con la que ocurre una situación de riesgo (evento de seguridad). En la Tabla 18 se muestran los valores adaptados para el nivel de exposición.

Tabla 18. Niveles de exposición

Exposición (E)	
Continua (100%)	4
Frecuente (60%)	3
Ocasional (30%)	2
Rara vez (10%)	1

Fuente: Autora

Puesto que para cada amenaza se manejan distintos niveles de riesgo, para calcular el grado de peligrosidad se tomó el promedio aritmético del producto de los factores P x I de cada columna en el mapa de riesgos, quedando la fórmula así:

GP = PROMEDIO ((P) x (I)) x (E)

Tabla 19. Grado de peligrosidad

GRADO DE PELIGROSIDAD = PROBABILIDAD (P) x IMPACTO (I) x EXPOSICIÓN (E) - Amenazas	
Valor Promedio (P x I)	**GP**
GP <= 4	Bajo
4 < GP <= 9	Medio
9 < GP <= 16	Alto

Fuente: Autora

[35] Evaluación de riesgos profesionales, método de William T. Fine. Grado de Peligrosidad. [Consultado 6 de Septiembre 2011]. Disponible en <http://white.oit.org.pe/ssos/documentos/cobertura_riesgos/secsoc/moduloiv/costos.html>

4.6.5. Tratamiento del riesgo

Cuando se han obtenido los niveles de riesgo y se han hecho los cálculos para evaluar los aspectos más importantes de los activos de información respecto a los incidentes, se debe definir el tratamiento que se le hará a cada activo de información. Según el autor Alberto G. Alexander "…se debe decidir cuáles acciones se han de tomar con esos activos de información que están sujetos a riesgos"[36].

En la ISO 27001:2005 se especifican cuatro opciones de tratamiento de riesgo. Para determinar qué acción se llevará a cabo para tratar el riesgo frente al activo de información, se debe tener en cuenta el nivel de prioridad del activo de información (que agrupa la probabilidad de ocurrencia y el impacto), el control implementado y la factibilidad económica de dicha acción. Esta decisión corresponde hacerla al responsable de cada activo de información, luego de haber evaluado los niveles de riesgo de cada uno de ellos y haber analizado el resultado del proceso de gestión de riesgos.

Reducción del riesgo. Para este caso, se deben implementar los controles necesarios para reducir el impacto al negocio de los riesgos (el nivel de riesgo, factor P x I) a un nivel aceptable –bajo-, el control implementado puede reducir el nivel del riesgo en uno de los dos factores; la probabilidad de ocurrencia o el impacto al activo de información. El resultado de ésta decisión es la Declaración de Aplicabilidad, que se completa con la gestión de riesgos y el análisis de brecha.

Aceptación del riesgo. Cuando no se hallan controles para reducir el riesgo, que no son efectivos para la mitigación de éste, o no pueden reducir ninguno de los factores del riesgo, se debe aceptar el riesgo. Esta situación se da cuando el nivel

[36] ALEXANDER, Alberto G. Diseño de un Sistema de Gestión de Seguridad de Información : Óptica ISO 27001:2005. Primera edición. Bogotá D.C. : Alfaomega Colombiana S.A., 2007. p 55.

de riesgo es bajo y no hay manera de reducirlo más, y resulta más costoso implementar un control que 'aprender a vivir' con el riesgo o las consecuencias del mismo. Esta decisión debe estar bien fundamentada, y se debe tomar teniendo en cuenta que el costo de aceptación no aumentará y los lineamientos en las políticas establecidas para la aceptación del riesgo.

Transferencia del riesgo. Esta opción se debe tomar cuando los niveles de riesgo son tan altos que es difícil para la empresa reducirlos, y tampoco es económicamente factible implementar controles para intentar reducir los factores de riesgo. Por lo tanto, transferir el riesgo significa que cambiará la responsabilidad del riesgo a un tercero (por ejemplo una aseguradora). Es importante definir cuánto del riesgo se transferirá a otra entidad, si ésta llevará la responsabilidad completa o una parte (hay que tener en cuenta que las aseguradoras suelen brindar mitigación en cuanto a impactos económicos). En conclusión, esta opción debe tomarse con prudencia y con apoyo de la Dirección.

Evadir el riesgo. Al evitar el riesgo se deben cambiar las actividades que lo originan[37] para eludir su presencia. Algunas de las formas para evitar el riesgo son: no llevar a cabo ciertas actividades del negocio, trasladar el activo de información a otra área o no procesar información sensible; por ejemplo, se tienen procesos de calidad, acciones preventivas y medidas de seguridad tecnológicas.

Toma de decisiones. La siguiente Tabla clarifica los criterios a tomar en cuenta para la decisión del tratamiento de riesgo, en base al diagrama del proceso de toma de decisiones para la elección de una opción de tratamiento[38].

37 ISO 27000, El portal de la ISO 27001 en español. [Consultado 6 de Septiembre 2011]. Disponible en <http://www.iso27000.es/sgsi.html#section2d>

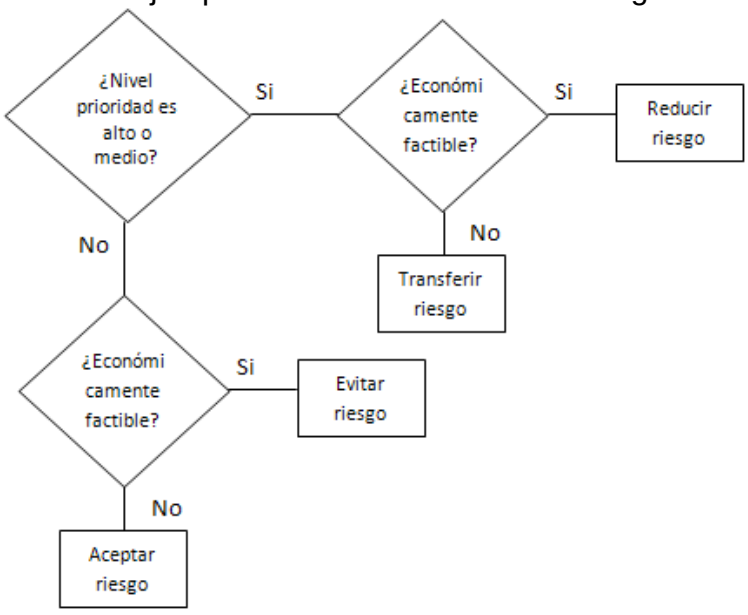
38 ALEXANDER, Alberto G. Diseño de un Sistema de Gestión de Seguridad de Información : Óptica ISO 27001:2005. Primera edición. Bogotá D.C. : Alfaomega Colombiana S.A., 2007. p 58.

Tabla 20. Criterios para las opciones de tratamiento de riesgo

Nivel Prioridad Activo Información	Factibilidad económica (implementar control)	Opción de tratamiento recomendada
Alto – Medio	SI	REDUCIR
Bajo	SI	EVITAR
Alto – Medio	NO	TRANSFERIR
Bajo	NO	ACEPTAR

Fuente: Autora

Figura 8. Diagrama de flujo opciones de tratamiento de riesgo



Fuente: ALEXANDER, Albert G.[39]; Autora

4.6.6. Riesgo residual

El riesgo residual es el que queda después de realizar el tratamiento de riesgos. Esto quiere decir que los riesgos se deben re evaluar en cuanto se lleven a cabo las acciones para su tratamiento (por ejemplo, implementar los controles); en tanto se actúa acorde al ciclo PHVA.

39 Ibíd, p 69.

Se debe tener en cuenta la eficacia de los controles que se han implementado para mitigar los riesgos. De la misma manera, se debe medir dicho indicador para aquellos que: fueron trasladados, se aplicó otra acción para evitarlos o se aceptaron.

A pesar de que la ISO 27001:2005 no exige calcular cuantitativamente el riesgo residual, sí busca el control y monitoreo sobre el riesgo remanente posterior a su tratamiento (los riesgos nunca estarán en un nivel cero) a través de su aceptación por parte de la Dirección. Se puede obtener el riesgo residual teórico teniendo en cuenta el valor del nivel de riesgo y el porcentaje de cubrimiento del mismo.

NOTA: Se hace referencia al cálculo de un riesgo residual *teórico*, ya que por ejemplo al cubrir la totalidad de un riesgo asegurando completamente un activo de información, el resultado sería cero. Sin embargo, en la práctica los riesgos no se pueden reducir a un valor nulo.

4.7. FASE 3: ESTABLECIMIENTO Y DIVULGACIÓN DEL SGSI

Esta fase se trata de hacer la preparación para implantar los controles. Esto implica generar las directrices de cómo se realizará el proceso, seleccionar los controles del Anexo A (Controles y Objetivos de Control) de acuerdo al resultado de la gestión de riesgos y estructurar y elaborar los procedimientos de gestión del sistema.

4.7.1. Políticas y objetivos de seguridad de información

La política de seguridad de información es la política general del SGSI sobre la cual la empresa enfoca sus actividades para gestionar la seguridad de información y emplea las directrices a cumplir por parte de todo el personal. Los objetivos

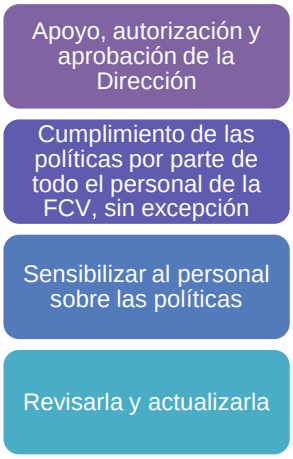
indican qué se pretende lograr al implementar un SGSI, pueden definirse los objetivos a corto, mediano y largo plazo.

Figura 9. Aspectos de la redacción de políticas de seguridad de información

Fuente: BORGHELLO, Cristian F[40].; Autora

40 Segu - info, seguridad de información. En: artículos. [En línea]. [Consultado 6 de Septiembre 2011] Disponible en <http://www.segu-info.com.ar/articulos/59-escribiendo-politicas-seguridad.htm>

Figura 10. Requisitos de una política de seguridad de información



Fuente: Autora

De conformidad con la ISO 27001:2005, debería existir un Manual de Seguridad de Información que establezca los objetivos y las políticas de seguridad de información, consolidadas en un único documento. Por lo tanto sería recomendable, para efectos de auditorías, que en un solo documento se definieran los objetivos, alcance y justificación de las políticas de seguridad de información, así como los activos de información que se protegerán (cómo y de quién).

ENTREGABLES: Manual de políticas de seguridad de información

4.7.2. Elaboración de la Declaración de Aplicabilidad

Como requisito de la ISO 27001:2005, se redacta la Declaración de Aplicabilidad, la cual contiene y explica los objetivos de control y controles del Anexo A de la norma que se seleccionaron, excluyeron y los que están actualmente implementados.

Los objetivos de la Declaración de Aplicabilidad son: seleccionar los objetivos de control y controles de acuerdo a los motivos de selección señalados, proporcionar

una visión clara y detallada de la implementación de los objetivos de control y controles (que respaldan los requisitos para proteger los activos de información), y relacionar la Declaración de Aplicabilidad con el Análisis Brecha, de manera que se clarifique el camino a seguir para la implementación de los controles planteado en el análisis de brecha.

En base al análisis realizado en el Análisis Brecha y de riesgos, se seleccionaron y excluyeron los controles del Anexo A que se implementarán, teniendo en cuenta la justificación de dicha decisión. Igualmente, se incluyeron aquellos controles ya implementados.

La implementación de cada control se había definido anteriormente en el Análisis Brecha; nuevamente se rectifica si se deben implementar o no de acuerdo a los resultados de la gestión de riesgos. En base a estas necesidades se creó un instructivo para seleccionar los controles (Ver Anexo 7).

ENTREGABLE: Declaración de Aplicabilidad

4.7.3. Registro de documentos de seguridad

Es importante saber con qué se cuenta actualmente. Por esta razón se debe registrar la documentación existente en la Dirección, Área o UEN de seguridad con la que se apoyan los procesos. Es muy común encontrar registros de los administradores o coordinadores de área importantes para el SGSI, pero que no se encuentran en un formato general corporativo.

4.7.4. Elaboración procedimientos de gestión

Los procedimientos de gestión son aquellos que proporcionan la base para el correcto funcionamiento del SGSI. Se pueden identificar estos procedimientos en

la elaboración de la Declaración de Aplicabilidad, pues la mayoría de estos son requisitos de la norma y se evidencian en los objetivos de control sobre la gestión de la seguridad de información.

Esto facilitará la diferenciación y clasificación de los resultados en la pirámide documental, y permitirá asignar claramente las responsabilidades por los procesos de gestión y las actividades propias de la Dirección.

4.7.5. Hitos

Es recomendable registrar las actividades realizadas por cada fase y sus hitos, para tener un orden y una evidencia de lo que se ha logrado. Es importante incluir los responsables de las tareas, los inconvenientes y las soluciones a estos.

Esto permitirá hacer un seguimiento claro y resumido del avance, pues en el momento de mostrar a los Directivos los resultados, la información simplificada y precisa proporcionará mayor acogimiento y aceptación.

4.8. FASE 4: IMPLANTACIÓN DEL SGSI

Llega el momento de implementar los objetivos de control, controles y políticas de seguridad. El objetivo de la fase es definir con alto nivel de detalle (quién, cómo, cuándo, cómo, con cuánto, por qué) el proceso de implementación de los controles seleccionados en la declaración de aplicabilidad.

4.8.1. Plan de tratamiento de riesgos

La necesidad de un plan de tratamiento de riesgos surge a partir de la continuación de la gestión de seguridad de información, en base a elaboración de una declaración de aplicabilidad donde se seleccionaron los controles (anexo A –

Controles y Objetivos de Control, ISO 27001:2005) con el fin de reducir los riesgos, siendo además un requisito del estándar.

El plan de tratamiento de riesgos (Ver Anexo 5) puede verse como un proyecto dentro del gran proyecto de implementación del SGSI; ya que, al tener un plan bien estructurado, es una excelente guía para la llevar a cabo las actividades que respaldarán la implementación de los controles, de una forma ordenada y precisa. Se tienen en cuenta los recursos, tiempos, responsables, hitos, entregables y actividades que se realizarán.

¿Por qué se elabora el Plan de Tratamiento de Riesgo en base a los activos de información y no de los riesgos?

Porque tiene como objetivo establecer las pautas, recursos y tiempos para implementar los controles que *reducirán* el riesgo. Esto, en términos de opciones de tratamiento de riesgos, quiere decir que se buscará disminuir o mitigar el impacto al negocio del activo de información dado un incidente de seguridad; ya que no es posible modificar la probabilidad de ocurrencia de algunas amenazas (por ejemplo, no se puede impedir un terremoto).

Al contar con una serie de controles o acciones determinadas para proteger los activos de información con mayores niveles de riesgo, se controlará uno de los factores que afectan dichos niveles. Teniendo en cuenta además que la gestión de riesgos elaborada está enfocada a los activos de información, las opciones de tratamiento de riesgo se tendrán en cuenta en base a éstos.

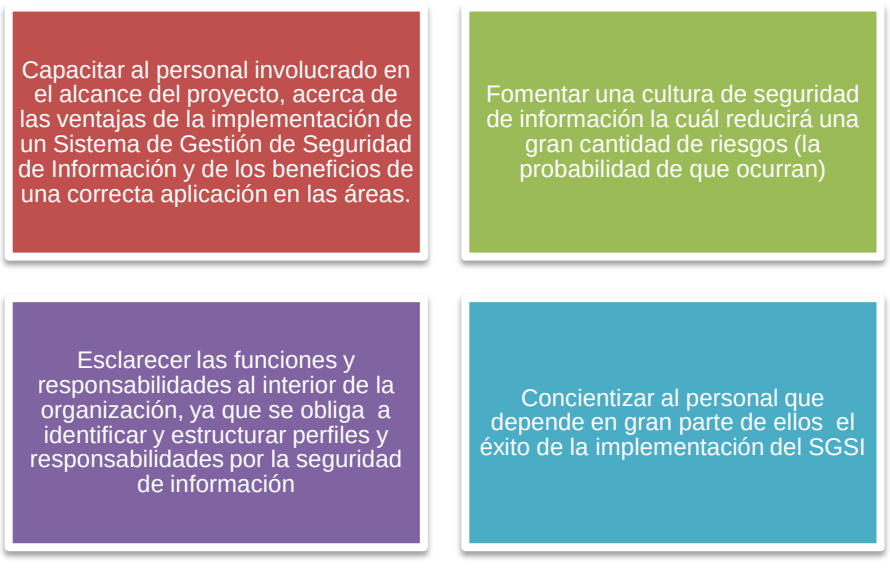
4.8.2. Planes de formación y concientización

Este es un de los puntos clave del proceso. Si las personas no conocen las políticas ni los procedimientos, ¿cómo se le puede dar marcha al SGSI?

La implementación de un SGSI implica la participación de todo el personal, pues se lleva a cabo un cambio a nivel organizacional enfocado a una cultura de seguridad de información, lo cual como todo cambio, puede generar choques si no se maneja adecuadamente y no se comunica ni se involucra al personal en el proceso. Se debe tener en cuenta que estos planes de concientización y formación se realizan en el proceso de cambio en la búsqueda de la gestión de la seguridad de información.

Cuando las personas se ven directamente involucradas en los grandes proyectos de la empresa, y son un factor activo e imprescindible en el proceso, colaboran y proponen mejoras. Esto hace que las probabilidades de alcanzar el éxito aumenten. Aunque la seguridad absoluta no existe, son evidentes los beneficios y resultados del trabajo y dedicación del personal. Es importante también tener en cuenta que los colaboradores pueden ser auditados; sin embargo, esta no debe ser la razón de ser de estos planes. La Figura 12 ilustra tales objetivos.

Figura 11. Objetivos de los planes de formación y concientización



Fuente: Autora

4.8.3. Implementar los controles

Esta etapa precisa tener cuidado y realizar reuniones con el personal, tanto para crear la documentación necesaria como para socializar los resultados y revelar las posibles correcciones en el proceso.

4.9. FASE 5: CONTROL Y SUPERVISIÓN DEL SGSI

El objetivo de la fase es medir la eficacia de la implementación de los controles, qué tantos cambios se realizaron, qué hace falta por hacer y si el plan de concientización y formación ha cumplido con su objetivo.

Esto se puede lograr obteniendo el valor de dos indicadores base: el pporcentaje de controles implementados y el porcentaje de documentos levantados y elaborados exigidos por la ISO 27001:2005.

Se contrastan los documentos y actividades realizadas para cada control, con lo que se definió anteriormente en la declaración de aplicabilidad, de manera que se puede visualizar qué cambios se hicieron y por qué.

Se deben llevar a cabo auditorías internas, grupos primarios, despliegue de documentos y acciones nuevas. También evaluar el cumplimiento de: las políticas del SGSI, los objetivos del SGSI y los objetivos de los controles en la declaración de aplicabilidad.

4.9.1. Detectar errores en la implementación de los controles

Es conveniente revisar en profundidad cada procedimiento, instructivo, registro, documento creado y acción o control implementado (a través de reuniones con los responsables de los activos de información y líderes de los procesos o jefes de

área). A medida que se avanza en el proceso de implantación de los controles, van surgiendo las fallas y se hacen evidentes los descuidos, pues ya se tiene más experiencia en el proceso y es más fácil detectar los errores.

Para lograrlo, los jefes de área y responsables por los activos de información deben realizar el seguimiento y revisión de la correcta aplicación de los procedimientos, instructivos y registros que se originan por el proceso de implementación de los controles. Esto se puede llevar a cabo mediante reuniones de grupo primario para definir responsabilidades y ajustes necesarios.

Para llevar a cabo un seguimiento de estos contratiempos, se deben advertir los cambios pertinentes realizados en el registro de hitos, especificando qué se modificó y a qué actividad o fase pertenece (Ver Anexo 25).

4.9.2. Detectar y registrar eventos e incidentes de seguridad

Si no existen, se deben crear los procesos para registrar y controlar los eventos de seguridad, de manera que en el caso de que llegase a ocurrir un incidente, exista un historial de las causas y eventos de seguridad. El área de Help Desk controla estos eventos por medio del registro de Tickets[41], y a través de estos se alimentan los indicadores de desempeño existentes que monitorean las actividades del proceso

4.9.3. Revisar los riesgos

Constantemente se hacen cambios en las organizaciones (de personal, de procesos, de infraestructura tecnológica, entre otros), y es importante adaptar el SGSI periódicamente a medida que ocurren. Por supuesto que no se llevarán a

41 Sistema de soporte técnico (hardware y software) basada en de solicitudes del cliente, que permite segregar las tareas por módulos del sistema y categorías de usuario. Administrado principalmente por el área de Help Desk.

cabo revisiones cada vez que se presente una novedad, pero para asegurar que el sistema de gestión esté funcionando bajo procesos reales y existentes, se debe supervisar el desempeño del SGSI y plantear las actualizaciones necesarias.

Esto se puede realizar por medio del estudio de los indicadores (métricas del proceso), la revisión del cumplimiento de los objetivos de los controles en la Declaración de Aplicabilidad y la verificación de que amenazas identificadas son consistentes con el análisis de riesgo realizado.

4.9.4. Auditorías internas

Este es un paso crucial para el control de un SGSI. Las auditorías permiten rectificar si se han cumplido los requisitos y objetivos planteados. Es importante tener en cuenta que el auditor no debe haber estado involucrado en el proceso, pues no se puede auditar el trabajo propio.

Uno de los controles de la ISO 27001:2005 señala que se deben realizar auditorías a los sistemas de información. Si bien la FCV cuenta con auditores en el Departamento de Planeación y Calidad y en el área de Auditoría, para llevar a cabo este tipo de procesos es necesario tener conocimientos específicos sobre sistemas de información y sistemas de gestión de seguridad de información.

4.10. FASE 6: MANTENIMIENTO Y MEJORA DEL SGSI

Se podría considerar como la fase final (la implantación de un SGSI es un proceso permanente), pero realmente se da paso al inicio de otro ciclo, y es la continuidad de la seguridad de información.

En esta etapa también se encuentra relación con la ISO 9001:2008, pues exige que se identifiquen, comuniquen, ejecuten e implanten acciones de correctivas,

preventivas y de mejora por medio de la creación de un procedimiento para su manejo y aseguramiento de la mejora continua.

La DTI cuenta con los procedimientos y registros para indicar y hacer seguimiento a los incidentes, por medio de los PHVA (así se conoce el registro de eventos, donde se mencionan los responsables, el tiempo de indisponibilidad del servicio, las acciones y decisiones tomadas, entre otros). El seguimiento de estas acciones permite el aprendizaje y la mejora en la realización de las actividades del proceso de implementación.

Al identificar estos hechos, se reevalúan las necesidades de la Dirección, Área o UEN. Esto implica analizar constantemente la situación y la conformidad con la norma, monitorear el comportamiento y adaptación del personal a los controles y nuevos procesos, revisar y re evaluar los riesgos, buscar otras formas de llevar a cabo los cambios (innovar) y establecer constantemente acciones de mejora. Este es un proceso que no se debe abandonar y debe permanecer en la continuidad.

5. PROYECTO DE IMPLEMENTACIÓN DE UN SGSI EN LA DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA DE LA FCV

En este capítulo se presentarán los resultados de aplicar el proceso explicado en el capítulo anterior. A medida que se avanzaba en el proceso de implementación del SGSI en la Dirección de Tecnología Informática, se creaban los entregables descritos en las fases de la metodología.

5.1. RESPONSABILIDADES

El equipo para el seguimiento de la seguridad de información se conformó por las siguientes personas:

- Líder del Proyecto: Ing. Jaider Fernando Rodríguez Lozano.
- Ingeniero Monitor: Ing. Leidy Viviana Ortiz.
- Analista de Seguridad: Silvia Margarita Diaz Diaz (Practicante. Autora).
- Comité de Seguridad de Información: Revisoría Fiscal, Auditoría, Director Tecnología Informática, Jefe Oficina Jurídica, Secretario General, Jefe Tecnología Informática, Jefe Administración de Proyectos, Jefe de Calidad, Ing. Monitor Calidad DTI.

Para efectos de la divulgación del proyecto de certificación con la ISO 27001:2005 para la Dirección de Tecnología Informática y sus avances, se conformó y se cambió el nombre del Comité de Seguridad Informática por el de Comité de Seguridad de Información, y se llevó a cabo la primera reunión de éste el día 30 de Noviembre de 2011.

5.2. ANÁLISIS DE LA SITUACIÓN ACTUAL – FASE UNO

Al iniciar la fase de análisis de la situación actual, faltaba claridad en algunos conceptos y en cómo se llevaría a cabo el proceso. El primer paso fue crear un cronograma por medio del cual se orientaría el desarrollo de las actividades (Ver Anexo 8). En el numeral 5.2.3 se esclarece el alcance, lo cual permite enfocar las tareas del proceso.

5.2.1. Información relevante de la Dirección

La Matriz de Flujo de Información se elaboró para todos los procesos de las UEN de la FCV, incluyendo los de la Dirección de Tecnología Informática. En el Anexo 9 se puede advertir el resultado del desarrollo de la identificación de la información saliente de los procesos. A partir de las Caracterizaciones de Proceso[42] se verificaron las salidas de cada actividad, y se listaron en la matriz.

Inicialmente se creó una matriz de actividades empresariales (con los procesos de entrada – actividad – procesos de salida), pero esta no llenaba las necesidades de la Dirección para identificar la información relevante.

5.2.2. Delimitación del alcance del SGSI

Esta etapa generó un poco de controversia al interior de la Dirección de Tecnología Informática, pues las opciones eran o incluir solamente la DTI o a toda la FCV; y por tanto se presentaron dos puntos de vista: por un lado, definir un alcance muy pequeño no está bien visto por un auditor, y es probable que no se acepte un alcance tan reducido. Pero por el otro lado la DTI se enfrentaba a un

42 Caracterización e Interacción del Proceso: Documento del Sistema de Gestión de Calidad que describe los objetivos, responsables, políticas, recursos, mediciones y actividades de cada proceso. Por ejemplo, el Departamento de Tecnología Informática es un proceso.

proyecto muy grande para abarcar toda la empresa, y al carecer de experiencia en la implementación de un SGSI se corría el riesgo de no tener éxito.

Para solucionar este inconveniente, se elaboró un diagrama de elipses de la interacción entre los procesos del Instituto del Corazón, lo cual evidenció que no era posible en este momento buscar la certificación de la FCV en su totalidad. Bajo la aprobación del Director de Tecnología Informática se decidió que se definiría un alcance relativamente pequeño y se ampliaría progresivamente para toda la FCV, pues la empresa es muy grande para implantar un sistema de gestión en un solo esfuerzo interno.

ALCANCE DEL SISTEMA PARA DTI.

Compromiso institucional. Este documento hace parte del Manual de Seguridad de Información, el cual describe y especifica el Sistema de Gestión de Seguridad de Información de una organización. Este documento define el compromiso, responsabilidades, autoridades y metodologías para cumplir con los requisitos del SGSI de la ISO 27001:2005[43]. De conformidad a las exigencias de la norma, establecida ésta (la definición del alcance) específicamente en la cláusula 4.2 Establecimiento y Gestión del SGSI, 4.2.1 a; se define el alcance del SGSI.

Objetivos

- El alcance del SGSI de la Fundación Cardiovascular de Colombia pretende determinar los departamentos, áreas, procesos de negocio y/o dependencias que abarcará el sistema.
- Por medio de este documento se especificarán los procesos implicados y excluidos, con las respectivas justificaciones de dicha decisión.

43 ALEXANDER, Alberto G. Diseño de un Sistema de Gestión de Seguridad de Información : Óptica ISO 27001:2005. Primera edición. Bogotá D.C. : Alfaomega Colombiana S.A., 2007. p 98.

- Identificar los procesos de negocio clave en base a los cuales se construirá e implementará un SGSI, de acuerdo a sus necesidades de seguridad.

Procesos implicados. El SGSI cubrirá los procesos de la Dirección de Informática y Tecnología de la FCV.

Desde el punto de vista del enfoque de proceso establecido en la norma ISO 27001:2005, DTI es un macro proceso en el cual se pueden identificar los Sub procesos según el esquema de procesos de negocio claves. Por lo tanto, el alcance es la disposición de un SGSI para los Procesos Propios de la Línea Básica[44]:

- Tecnología Informática. Proceso en el que se documenta la Administración de Software, Hardware y la Infraestructura tecnológica para mantener el sistema de información disponible y seguro.

- Administración de Proyectos. Proceso en el que se documenta la planeación y el control de los proyectos, tanto de mantenimiento de aplicaciones actuales como a nuevas tecnologías.

- Help Desk. Proceso en el que se documenta las directrices a tener en cuenta para generar no solo un producto de calidad sino que satisfaga las necesidades de los usuarios.

- Diseño y Desarrollo. Proceso en el que se documenta las etapas de construcción y mantenimiento del software, garantizando la calidad e integridad de la información.

44 Procesos definidos por el Sistema de Gestión de Calidad

Se seleccionan estos procesos con el fin de establecer un alcance limitado que permita a la organización adaptarse al estándar (ISO 27001:2005), dando paso a un proceso de implantación del SGSI eficaz y eficiente, proveyendo una culturización a nivel organizacional respecto la norma y su importancia. Y ya que DTI es el principal responsable por el tratamiento y resguardo de información, éste ha sido elegido como alcance inicial del SGSI.

Este alcance está alineado con las actividades de la empresa ya que la Dirección de Informática y Tecnología brinda servicios operativos a todas las UEN y demás áreas de la FCV. También, DTI es responsable por la producción de conocimiento, servicios y productos (software) importantes para el funcionamiento y continuidad del negocio.

El éxito de la implantación del SGSI en este alcance impulsará la ampliación del mismo, y por lo tanto, se llegará gradualmente a cubrir toda la organización.

Terceros y externos. Dado que el alcance se limita a una gran Dirección de la empresa, los procesos que actúan como procesos de apoyo y que tienen alguna interacción con los del DTI, no son procesos externos como tal.

Los procesos de las UEN son considerados externos, como si fuesen organizaciones extrínsecas. Esto debido a que el alcance delimita una 'zona segura', la cual debe proteger el flujo de información desde ésta zona a entidades externas ('zona no segura'); por lo tanto, aunque los procesos de las UEN y los procesos de DTI pertenezcan a la misma organización, en el intercambio y manejo de información debe haber una diferenciación clara.

La información que sale de la 'zona segura' debe ser tratada de manera especial, según se implementa el SGSI, aún cuando se trate de la misma organización.

Procesos excluidos. Los procesos que se mencionarán a continuación se interrelacionan con los procesos del alcance (procesos implicados). Por lo tanto se toman como procesos de la organización que interactúan con los del DTI.

- Procesos de mejoramiento
- Procesos de apoyo administrativo

Estos procesos fueron excluidos del alcance del SGSI debido a que sus actividades interactúan con los procesos incluidos en el alcance pero, no pertenecen a ellos y actúan como apoyo y mejora.

Procesos de la línea básica de operaciones de las UEN:

- FCV Comercializadora
- FCV Telemedicina
- FCV Bioingeniería
- FCV Eventos y Mercadeo
- FCV Administración Hospitalaria
- FCV Universidad Corporativa
- FCV Institutos del Corazón Sedes Floridablanca, Santa Marta, Manizales e Ibagué
- FCV Productos Hospitalarios

Estos procesos han sido excluidos porque se desea aprovechar al máximo la eficacia de la implantación del SGSI, y para esto es recomendable acotar el alcance –inicialmente- a un proceso clave en la organización, y asegurar la eficacia y eficiencia del proceso de implantación del SGSI.

Localizaciones físicas. Las localizaciones físicas que abarca el SGSI son:

- Oficinas de la DTI en el Centro Tecnológico Empresarial.
- IT Room CTE (Cuarto de procesamiento).

Sistemas de información. Los sistemas de información involucrados en el sistema de soporte a las actividades diarias de los procesos.

- SAHI.[45] Sistema de Administración Hospitalaria Integrado, es un software desarrollado por la Fábrica de Software de la FCV. Actualmente la aplicación está instalada en 20 hospitales del país. Contiene gran cantidad de módulos, entre ellos la Historia Clínica Electrónica, administración de cartera, personal, contabilidad y activos fijos, entre muchos otros.

Interfaces del SGSI. La interacción entre los procesos se llevó a cabo por medio del diagrama de elipses de procesos (Ver Anexo 10).

Marco legal. El marco legal vigente y aplicable para los procesos de la Dirección de Tecnología Informática se encuentra en el Anexo 24.

5.2.3. Registro de activos de información

Teniendo en cuenta la Matriz de Flujo de Información y el Documento del Taller de Activos de Información creado por el abogado Dr. Arean Velasco[46], se elaboró el Formato para el Registro de Activos de Información de la FCV y se recopiló y organizó la información para alimentar dicho registro (Ver Anexo 16), siguiendo los lineamientos descritos en el capítulo cuatro (numeral 4.5.2). Este registro es un requisito exigido por la norma, y tuvo gran acogida por la Dirección de Tecnología Informática, ya que muestra de forma ordenada los activos de información de la empresa.

45 FUNDACIÓN CARDIOVASCULAR DE COLOMBIA. En: Software en Salud. [En línea]. [Consultado 14 Enero 2012]. Disponible en < http://www.fcv.org/descargar/BrochureSahi.pdf>

46 Consultor experto en protección de datos personales, derechos de autor y seguridad de información; de la firma Velasco & Calle D'Aleman, con contrato de prestación de servicios profesionales y asesoría experta para la FCV.

5.2.4. Brecha existente

Se analizó la diferencia existente de la situación actual de la DTI en cuanto a los requisitos de la norma, por medio de la matriz elaborada (Ver Anexo 15).

Según la ISO 27001:2005: '…el término "procedimiento documentado"…, significa que el procedimiento está establecido, documentado, implementado y mantenido'[47]. Por lo tanto, según la norma, todo control que no esté documentado o le falte algún aspecto para su adecuada implementación, no está implantado. De acuerdo a la Matriz del Análisis Brecha, se tiene:

Tabla 21. Implementación de controles

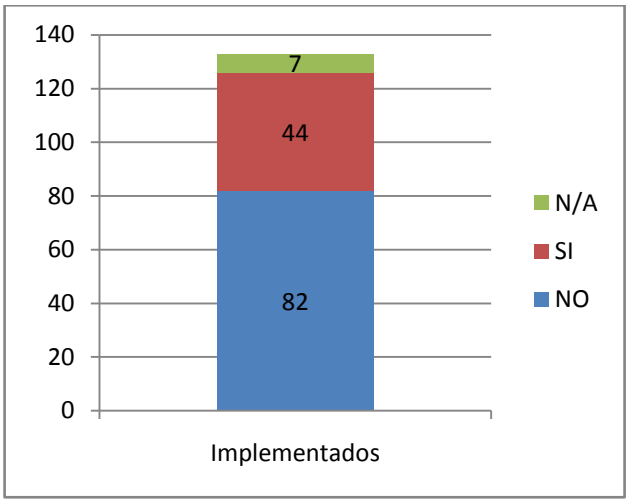
# Controles	Implementado	% (sobre 133 controles)
82	NO	61,654
44	SI	33,082
7	N/A (No Aplica)	5,263

Fuente: Autora

De acuerdo a esta tabla, más de la mitad de los controles no están implementados, pero no es un panorama desalentador, pues no es necesario comenzar de cero y además esto refleja la conformidad de la FCV con un sistema de gestión (ISO 9001:2008).

47 ALEXANDER, Alberto G. Diseño de un Sistema de Gestión de Seguridad de Información : Óptica ISO 27001:2005. Primera edición. Bogotá D.C. : Alfaomega Colombiana S.A., 2007. p 140.

Figura 12. Número de controles implementados



Fuente: Autora

Puesto que el porcentaje del 61,65% de -controles no implementados- no es de gran ayuda para analizar la situación actual frente a los controles, para ampliar la visión del nivel de implementación se establecieron las categorías por colores anteriormente mencionadas y clasificadas en la Tabla 22.

Tabla 22. Número de controles por nivel de implementación

No. Controles	Id	Característica	Porcentaje [%]
7	No aplican	--	5,26
21	Púrpura	Falta implementación del control	15,78
11	Verde	Falta documentar el control (sí está -bien- implementado por completo)	8,27
44	Azul	Sí está implementado	33,08
3	Naranja	Planificado o en proceso (por el proceso de implementación)	2,25
47	Rojo	No implementado	35,33

Fuente: Autora

La finalidad de estas categorías no sólo es mostrar los controles no implementados, sino también aquellos que tienen algún nivel de implementación o

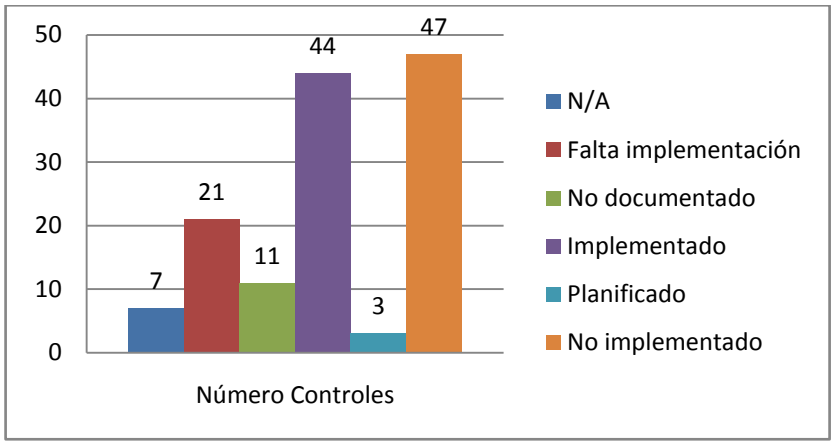
deben mejorar algún aspecto; de manera que se puede percibir claramente qué falta, qué se debe hacer y cómo, y así llevar a cabo el proceso de implantación eficientemente, sin tener que volver a analizar los controles e implementar desde cero los que ya llevan un avance definido.

De esta tabla se puede inferir que de un total de 82 controles NO implementados, 35 tienen algún nivel de avance (11 faltan por documentar, estando ya implementados, 21 requieren mejoras y 3 están en proceso), para los cuales el proceso de implantación será más eficiente, y de igual manera se cumplirá con los objetivos.

Los controles que no aplican (N/A) tienen su razón por no tener relación con las actividades de la empresa, ni las que se manejan en la Dirección de Tecnología Informática (esto daría un total de 126 controles realmente aplicables para la FCV y específicamente DTI). Los controles identificados con el color naranja están en actual proceso de implementación por el proceso que se está llevando a cabo para la implantación del SGSI.

Un 33% corresponde a los controles no implementados en ningún nivel, y que aún no están en proceso; esto deduce que menos de la mitad de los controles deben ser implantados desde un nivel cero.

Figura 13. Número de controles por categoría



Fuente: Autora

CONCLUSIONES ANÁLISIS BRECHA

Se encontró un buen nivel actual de implementación de los controles, por tanto no hay necesidad de comenzar de cero para cada objetivo de control.

Los controles que requieren mejora, ajuste o complementos, tienen sus recomendaciones en la matriz de Análisis de Brecha; esto puede brindar eficiencia en el proceso y facilitar a los responsables esta labor.

Este análisis permite clarificar la situación actual de la FCV frente a los controles de la ISO 27001:2005, lo cual proporciona más herramientas para la implementación de los controles.

Una buena base para el proceso de implantación de controles es la norma ISO 27002:2005, la cual debe ser revisada cuando se lleve a cabo nuevamente un análisis de brecha.

5.3. INFORME DE LA GESTIÓN DE RIESGOS – FASE DOS

Siguiendo la metodología elaborada, se completó el Mapa de Riesgos para los activos de información de la Dirección de Tecnología Informática (Ver Anexo 17), igualmente la matriz de amenazas y vulnerabilidades (Ver Anexo 6); y el Informe de medición y análisis del riesgo el cual se detallará en esta sección.

ALCANCE DEL ANÁLISIS DE RIESGO

Todos los procesos de la Dirección de Tecnología Informática: Departamento de Tecnología Informática, Administración de Proyectos y Calidad y Help Desk.

PERSONAS ENTREVISTADAS

- Ing. Jaider Rodriguez Lozano – Jefe Departamento Tecnología Informática
- Ing. Leidy Viviana Ortiz – Ingeniera Monitor de Calidad DTI
- Ing. Diana Marcela Sanabria – Administradora de Redes DTI
- Ing. Andrea Lizeth Fuentes – Administradora de Base de Datos DTI
- Ing. Jhoan Orlando Bueno – Analista Help Desk
- Ing. Areli Afanador – Arquitecta de Software

RESULTADOS

Niveles de Riesgo. Para resumir el resultado de los niveles de riesgo, en la siguiente tabla se muestra su frecuencia por rangos.

Tabla 23. Frecuencia niveles de riesgo

Nivel Riesgo	Rangos NR	Frecuencia	[%]	Nivel Riesgo
BAJO	1	68	1,98	BAJO
	2	328	9,53	
	3	518	15,06	
	4	774	22,50	
MEDIO	6	452	13,14	MEDIO
	8	580	16,86	
	9	60	1,74	
ALTO	12	360	10,47	ALTO
	16	300	8,72	

Fuente: Autora

Relación tasación activos de información – cálculo nivel de riesgo. El promedio aritmético de los valores de confidencialidad, disponibilidad e integridad corresponde al valor que se utiliza en el mapa de riesgos para calcular el nivel de riesgo, siendo el factor de impacto al negocio (I). Esta relación se da debido a que las fallas o pérdidas de estas propiedades en un determinado activo de información, definen el nivel de la consecuencia que genera en la empresa; que en los términos utilizados se conoce como el impacto.

En la siguiente figura se visualiza un ejemplo de la tasación de activos de información dentro del formato utilizado.

Figura 14. Ejemplo tasación de un activo de información: Servidor de datos

Activo de información	Niveles			Total	Responsable	Líder
	Disponibilidad	Integridad	Confidencialidad			
Servidor de BD	4	3	4	3	DTI	Jefe DTI

Fuente: Autora

Nivel de prioridad del activo de información. Se calculó teniendo en cuenta el promedio aritmético de todos los niveles de riesgo por activo de información (filas

del mapa de riesgos). Ya que la mayoría obtuvo un nivel cualitativo igual a “medio”, se analizarán los valores cuantitativos (Ver Anexo 11).

Porcentaje de amenazas por tipo. La siguiente tabla muestra el porcentaje de amenazas a los activos de información por tipo.

Tabla 24. Porcentaje amenazas por tipo

Tipo amenaza	Porcentaje [%]
Tecnologías Informáticas	34,884
Social	18,605
Física	11,628
Recurso humano	11,628
Legal	8,14
Eventos natural	8,14
Operacional	6,977

Fuente: Autora

ANÁLISIS

Activos de información prioritarios. De acuerdo a la información en el documento Registro de Activos de Información (Ver Anexo 16), la mayoría de aquellos que fueron clasificados en la categoría *Datos confidenciales* (compañía o clientes) y *privados* son los que mayor nivel de prioridad poseen.

A partir de estos datos se no se puede obtener mayor conclusión, ya que cerca del 95% clasificaron como medianamente prioritarios, por lo tanto, se debe llevar a cabo otro tipo de análisis para clarificar cuáles activos de información son más vulnerables, excluyendo los que obtuvieron un valor no significativo para el nivel de prioridad.

Tipos de amenazas con mayor exposición. La exposición de la amenaza es la frecuencia con la que ocurre (o puede ocurrir) un incidente o situación de riesgo. Este factor determina el grado de peligrosidad de la amenaza.

Las amenazas con mayor exposición son las del tipo de Tecnologías Informáticas; que cuentan con un 76.67% de ellas en nivel alto del grado de peligrosidad. Por lo cual se infiere que las principales vulnerabilidades a ataques se encuentran en aspectos tecnológicos.

Las amenazas de tipo Física y de Recurso Humano cuentan ambas con un 60%. Las vulnerabilidades en el aspecto humano de una organización pueden tener un impacto alto, pues depende en gran parte del personal el manejo y custodia de los activos de información.

Análisis de riesgo excluyente por Grado de Peligrosidad de amenazas. Otro planteamiento que se realizó para el análisis de riesgos fue eliminar los tipos de amenazas con los grados de peligrosidad más bajos. Teniendo en cuenta esto, y al observar el mapa de riesgos, se concluye que las amenazas de tipo social, legal y evento natural se pueden omitir para éste análisis.

La justificación de este proceso es analizar la prioridad de los activos de información y el grado de peligrosidad de un riesgo teniendo en cuenta las amenazas que mayor exposición tienen. El objetivo de excluir ciertos tipos de amenazas se basa en que éstas no causan consecuencias graves a los activos de información, por lo que el nivel de riesgo es bajo. (Esta exclusión se hace únicamente para hacer este análisis, no para tomar las decisiones en el plan de tratamiento de riesgos).

GRÁFICAS

Las tablas y gráficas de los resultados y análisis de riesgos se encuentran en los Anexos de este documento.

- Promedio nivel de prioridad activos de información (ejemplos) – Anexo 11
- Análisis excluyente: Grados de peligrosidad altos – Anexo 12
- Promedio nivel de riesgo activos de información críticos (ejemplos) – Anexo 13
- Grado de peligrosidad de cada tipo de amenazas – Anexo 14

CONCLUSIONES

Los activos de información que son considerados confidenciales para la empresa, requieren de niveles más altos de disponibilidad, integridad y confidencialidad, por lo tanto; son los más vulnerables y prioritarios en el momento de tomar las decisiones de tratamiento de riesgo.

Las amenazas de tecnologías informáticas tienen los niveles más altos de exposición al riesgo, lo cual quiere decir que son las que ocurren con más frecuencia y más perjudiciales pueden ser para los activos de información.

Una buena parte de los niveles de riesgo son bajos, por lo tanto la decisión del tratamiento de riesgos probablemente no requerirá de gran inversión económica para la protección de algunos de los activos de información, sin embargo; se deben tener en cuenta los criterios establecidos en la metodología de gestión de riesgos para dicha evaluación.

5.4. DIVULGACIÓN DEL SISTEMA – FASE TRES

Las políticas de seguridad de información no fueron redactadas a partir de cero. Para lograr como resultado el Manual de Políticas de Calidad y Seguridad de Información, se comenzó por unificar dos documentos: el del Manual de políticas de calidad, confiabilidad y seguridad informática y el de las políticas de Seguridad e Integralidad de la Información. A partir de estos documentos, se fueron escribiendo las políticas que soportarían la implementación de los controles.

5.4.1. Contenido del manual de políticas de seguridad

Debido a que se trata de un documento que define las directrices de la FCV para sus estándares de calidad y seguridad de información, su contenido es de interés interno y confidencial. Se mencionará el contenido (índice) del manual:

- Objetivos del manual
- Alcance
- Definiciones
- Políticas de seguridad de información
- Procesos relacionados
- Requisitos legales aplicables
- Contenido del manual
    - Políticas de responsabilidad sobre la seguridad de información
    - Políticas de seguridad de información de la DTI
    - Políticas de seguridad informática
    - Políticas y lineamientos para el uso de equipos de cómputo y recursos informáticos y de telecomunicaciones
    - Políticas y lineamientos para el uso del servicio de internet, correo electrónico, mensajería instantánea, telefonía y videoconferencia
    - Políticas para buen uso y transmisión de la información

- Políticas para el control de acceso físico y lógico
- Políticas y lineamientos para la custodia y seguridad de la historia clínica electrónica
- Política de revisión del manual

5.4.2. Objetivos del SGSI

Corto plazo. Asegurar la eficacia del proceso del plan de implementación del estándar internacional ISO 27001:2005 en conformidad a los requisitos de la misma y al marco legal aplicable vigente.

Elaborar una estrategia eficiente de implementación con el fin de ampliar el alcance del Sistema de Gestión de Seguridad de Información en base a un caso de éxito dentro de la Dirección de Tecnología Informática de la Fundación Cardiovascular de Colombia.

Promover una cultura de seguridad de información en todo el personal de la Dirección de tecnología Informática.

Mediano plazo. Fortalecer los procesos de gestión de la FCV buscando la integración de la información y de los procesos en todas las áreas corporativas.

Obtener la certificación ISO 27001:2005 para el alcance definido actualmente: la Dirección de Tecnología Informática.

Largo plazo. Brindar a los clientes y proveedores calidad y seguridad en los servicios bajo altos estándares.

Preservar la imagen corporativa de la Fundación Cardiovascular de Colombia y ser una empresa líder en cumplimiento de la seguridad de información en el país.

5.3.3. Declaración de Aplicabilidad

El desarrollo de la Declaración de Aplicabilidad (DdA) fue un proceso de constantes reuniones, profundización del tema y revisiones. Se elaboró también el instructivo para la selección de controles (Ver Anexo 7), y resultó una Declaración de aplicabilidad muy completa, distinta a la de los formatos que se pueden encontrar en línea.

En el Anexo 18 se puede encontrar la DdA para la Dirección de Tecnología Informática. Este documento debe ser revisado periódicamente, con el fin de medir la eficacia de los controles, el proceso de implementación y el cumplimiento de los objetivos; de manera que se actualice y se detallen los cambios realizados.

5.4. IMPLEMENTACIÓN DE LOS CONTROLES – FASE CUATRO

A medida que se avanza en el proceso de implementación la exigencia es mayor, puesto que se ponen a prueba los conocimientos adquiridos y la fortaleza de la etapa de planificación. Es importante mantener contacto constante con los jefes de área y responsables de los activos de información, ya que de ellos depende que los resultados producidos sean correctos y sí correspondan a las necesidades establecidas.

5.4.1. Plan de tratamiento de riesgo

En el mapa de riesgos, en el cual se calcularon los niveles de riesgo para cada activo de información, se evaluaron las opciones de tratamiento en base a la factibilidad económica de implementar un control y al nivel de prioridad del activo de información; para la mayoría de estos la opción de tratamiento fue reducir (esto quiere decir que se debía seleccionar un control del Anexo A, lo cual dio resultado a la Declaración de Aplicabilidad).

Ya teniendo clara la forma como se tratará el riesgo, se procede a crear el plan. La realización del Plan de Tratamiento de Riesgo (PTR) se hizo con apoyo de: el registro de activos de información, la declaración de aplicabilidad, el mapa de riesgos, la ISO 27002 y las consultas bibliográficas.

El enfoque de la aplicación de los controles se basará en los procesos (y sus actividades) que conciernen a la Dirección de Tecnología Informática (DTI). Así, por ejemplo, en el control sobre seguridad de los recursos humanos, se gestionarán los procedimientos que tienen relación directa con las actividades y responsabilidades de la DTI. Si en el proceso de selección de personal DTI está encargado de crear las cuentas de usuario y asignar permisos, estos serán los procedimientos mencionados.

En el Anexo 19 se encuentra el PTR elaborado para la Dirección de Tecnología Informática.

5.4.2. Planes de formación y concientización

El orden en el que se llevarán a cabo los planes de formación y concientización en la DTI será de la siguiente forma:

Tabla 25. Proceso formación y concientización

Concientización	- Comunicación del proyecto - Conocimiento - Sensibilización	Objetivo: dar a conocer al personal las intenciones de implementar un SGSI, de qué trata este proceso y cómo se llevará a cabo
Formación	- Aprendizaje - Capacitación - Puesta en práctica, desarrollo de tareas	Objetivo: participación activa del personal, capacitaciones y definición de responsabilidades y resultados esperados del proceso

Fuente: Autora

Claves para los planes de concientización y formación

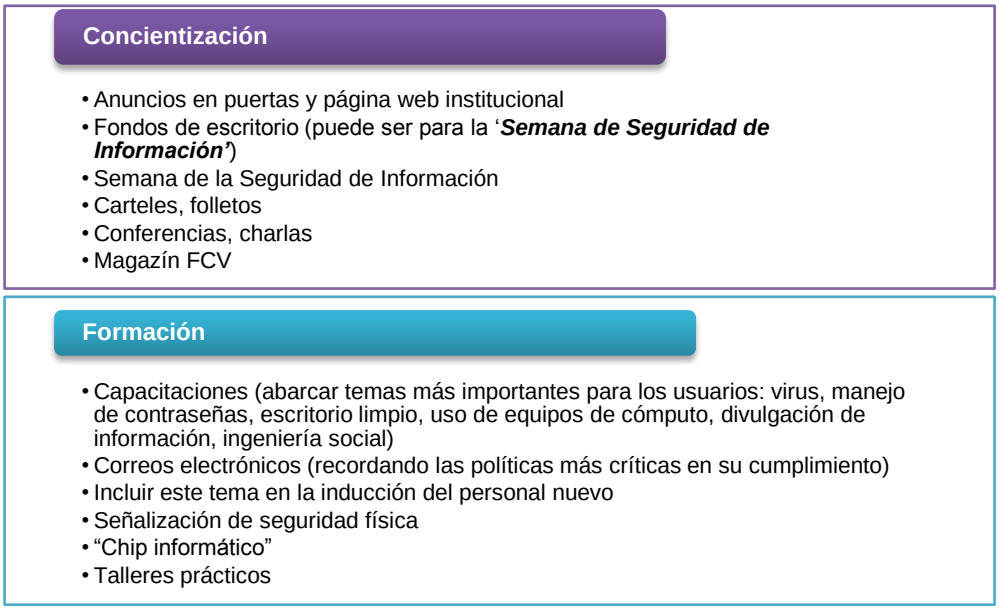
- Comunicación (escuchar y opinar)
- Impactar
    i. Ser claro
    ii. Reforzar
    iii. Políticas bien estructuradas
- Personal involucrado
- Recursos y material disponible para la formación (documentación, normas, artículos, diapositivas, capacitaciones)
- Cambio cultural
    i. Perseverancia y paciencia
    ii. Enseñanza y comunicación continua
    iii. Apoyo de la Gerencia.

Preliminar. Es necesario infundir una cultura de seguridad de información. Se involucra al todo el personal de la DTI incluido en los procesos del alcance. La importancia de estos planes de concientización y formación radica en que, de nada sirve montar un SGSI si las personas que deben ejecutar los procedimientos, seguir las políticas y disminuir el impacto de los riesgos no saben cómo ni por qué hacerlo, y mucho menos sin saber de qué se trata.

Por lo tanto, el primer paso es dar a conocer al personal involucrado la intención de implementar un SGSI, la razón por la cual se llevará a cabo éste proceso, cómo se realizará y por qué es tan importante la participación activa de todos los usuarios.

Diseño de campaña. Se proponen actividades y medidas para concientizar y formar al personal.

Figura 15. Actividades de formación y concientización



Fuente: Autora

Contenidos

Tabla 26. Contenidos para divulgación del SGSI

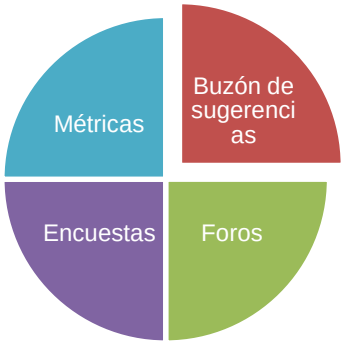
Charla	Objetivo	Contenido
De sensibilización	Dar a conocer el concepto de un SGSI y el propósito de implementarlo	Qué es un SGSI
		Por qué se implementa un SGSI
		Cuál es la importancia de la seguridad de información en la DTI
		¿Qué tiene que ver conmigo?
		"Acá no sucederá", "Es sólo tarea de DTI"
De motivación	Motivar al personal para que participe, se interese en el tema y en un futuro guíe sus acciones en base a la seguridad de información.	Objetivos de la DTI (más adelante de la FCV cuando se extienda el alcance) frente al SGSI
		Qué es la seguridad de información
		Alcance definido y principales riesgos
		Buenas prácticas

De Información	Capacitar e informar respecto a los puntos más elementales de la seguridad de información que involucran acciones humanas.	Virus
		Manejo de Contraseñas
		Uso correcto de equipos de cómputo
		Escritorio Limpio
		Ingeniería Social
		Correos Electrónicos
		Divulgación de Información

Fuente: Autora

Mecanismos de monitoreo y evaluación. Para asegurar la eficacia y avance de los planes de concientización y formación, y qué tanto se ha infundido en la cultura organizacional la seguridad de información, es importante realizar retroalimentación del proceso. Para esto se pueden tener en cuenta distintos métodos que ayudarían a los encargados de la gestión de la seguridad de información a obtener una curva de aprendizaje, evaluando los aspectos más importantes para realizar cambios a la estrategia elaborada.

Figura 16. Mecanismos de monitoreo y control



Fuente: Autora

5.4.3. Implantación de los controles

Los controles seleccionados en la Declaración de Aplicabilidad fueron implantados en esta etapa. Se culminó la elaboración del Manual de Políticas de Calidad y

Seguridad de Información, se crearon los procedimientos, instructivos y registros que soportan las actividades que se llevan a cabo en el Departamento de Tecnología Informática, y por último se obtuvo la aprobación del Jefe de Tecnología Informática para subir estos documentos a la página de calidad de la FCV.

5.5. CONTROL Y MEJORA CONTINUA DEL SISTEMA

Para continuar con el proceso de implementación del SGSI en la Dirección de Tecnología Informática, es necesaria la aprobación de un presupuesto por parte de la Dirección Ejecutiva con el fin de llevar a cabo una pre auditoría con el ICONTEC e implantar los controles faltantes, ya que algunos requieren de recursos para poder completar el proceso.

Sin embargo, para efectos de revisión de la eficiencia de la estrategia desarrollada y la metodología aplicada, se comparan dos indicadores principales:

1. Porcentaje de controles implementados
2. Documentos levantados y elaborados exigidos por la ISO 27001:2005

El primer indicador se compara con el valor inicial obtenido a partir del análisis de brecha[48]: 33,08% controles implementados (44). Al finalizar la cuarta fase, este número incrementó a 74,44% (99). Esto da un total de 27 controles **no** implementados[49] (23% de no conformidad).

Respecto al segundo indicador, el valor inicial se obtiene de la documentación base exigida por la norma. En el Anexo 20 se definieron estos documentos, y de

48 Tabla 21, p 83.
49 133 controles en total – 7 controles que no aplican – 99 implementados = 27 no implementados

conformidad a ellos, la DTI alcanzó un total de 29/77 (37,66%) previo al proceso de implementación. Al finalizar la fase cuatro, se encontró un 61/77 (79,22%).

La determinación de los valores de estos indicadores es parte de la pre auditoría que ha de realizar la entidad certificadora, y la estimación hasta ahora obtenida evidencia que la metodología elaborada y aplicada fue eficaz, mostrando un nivel de satisfacción alto en el proceso de implementación.

Tabla 27. Indicadores de eficacia

Indicador 1		**Indicador 2**	
Antes	Después	Antes	Después
33,08%	74,44%	37,66%	79,22%

Fuente: Autora

Por otro lado, las dos últimas fases (cinco y seis) deben ser ejecutadas por el equipo de seguridad de información, haciendo seguimiento de la efectividad de la implementación de los controles y la gestión de riesgos. Las auditorías internas también son necesarias, pero para esto se necesita un mayor nivel de madurez en la seguridad de información en la empresa, de manera que el Departamento de Planeación y Calidad se pueda encargar de estas actividades.

La Dirección debe estar al tanto de los avances del proceso al igual que el Comité de Seguridad de Información, ya que para realizar cambios, mejoras y otras modificaciones, se requiere de su previa aprobación y apoyo.

6. PIRÁMIDE DOCUMENTAL DEL SGSI EN LA DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA

Gran parte de la evidencia del proceso de implementación se condensa en documentos. Los sistemas de gestión requieren documentación del proceso, pues es esto lo que soporta el cumplimiento de los requisitos y las actividades que se están llevando a cabo para dicho fin; también son el sustento que tienen las empresas para enfrentarse a una auditoría.

6.1. NIVELES DE LA DOCUMENTACIÓN

De acuerdo a las actividades realizadas en la Dirección de Tecnología Informática se elaboró la pirámide documental (Figura 18), teniendo en cuenta los requisitos de la norma, los procesos y necesidades de la DTI.

Figura 17. Pirámide documental DTI

Fuente: Autora

Nivel 1: Manual de Políticas de Calidad y Seguridad de Información. Los documentos de este nivel establecen el marco bajo el cual se guiará el proceso,

son el “padre” de los demás niveles. Contiene las políticas y objetivos del sistema y de seguridad de información, así como las directrices para establecer los estándares de calidad en el manejo, procesamiento y almacenamiento de información. También incluye las responsabilidades de los líderes de los procesos (jefes de área) y el marco legal vigente aplicable.

Las políticas se integraron en este manual con el objetivo de facilitar su revisión, seguimiento y mantenimiento. No se vio necesario que el manual incluyera el alcance, la metodología de gestión de riesgo y la declaración de aplicabilidad, pues esto extendería demasiado el documento y ya no se prestaría para una lectura cómoda, ya que los usuarios del sistema de gestión deben leer las políticas.

Nivel 2: Documentos de gestión del SGSI. Son aquellos documentos exigidos por la norma y procedimientos que soportan la implementación del sistema de gestión de seguridad de información. Estos definen la forma como se dirigirán las actividades de seguridad de información y sentará las bases para la administración del sistema.

Entre ellos se encuentran procedimientos para la implementación del SGSI, para la clasificación de activos de información, selección de controles y la metodología de gestión del riesgo. Otros documentos requeridos: alcance del sistema, el plan de tratamiento de riesgo y el informe de medición de riesgo.

Nivel 3: Procedimientos e instructivos de actividades. En este nivel se encuentran todos los procedimientos e instructivos que dan apoyo a la realización de las actividades propias de la DTI. Describen cómo se debe llevar a cabo determinada tarea, lo cual es necesario para demostrar que éstas se efectúan en un orden establecido, con responsabilidades y recursos definidos y referencian la documentación necesaria de soporte para una auditoría.

Los instructivos para manejo de software, mantenimiento de equipos, elaboración de copias de seguridad y administración de dispositivos hacen parte de este nivel.

Nivel 4: Registros y anexos soporte. Los registros son los soportes y las evidencias de que se está cumpliendo con un requisito de la ISO 27001:2005 y de que se están llevando a cabo las actividades definidas en los instructivos y procedimientos. Los registros y anexos deben estar referenciados por un procedimiento y/o instructivo, pues en la mayoría de casos el soporte de éstos es un registro.

Es importante analizar desde el punto de vista de los requisitos de la norma, los procesos y sus actividades en el momento de elaborar los documentos, pues si previo a esto no se encuentra una consistencia entre los factores mencionados, se puede caer en una documentación mecánica, donde se elaboran documentos a medida que aparece un requerimiento nuevo sin evaluar a dónde pertenece.

6.2. RELACIÓN Y REQUISITOS

Como se mencionó anteriormente, antes de crear un documento se debe determinar a qué proceso apoya y qué actividades soporta. En base a esto, se organizaron los resultados y evidencias de la implementación de los controles por medio de una lista de chequeo, que relaciona el proceso al que pertenece y facilita el seguimiento de la documentación desde su procedencia.

También se mostrará en esta sección un compilado elaborado de la documentación exigida por la ISO 27001:2005 y el nivel de conformidad de la DTI a esta.

6.2.1. Evidencias del proceso de implementación

Se elaboró un registro de la documentación desarrollada a lo largo de la práctica teniendo en cuenta los niveles definidos anteriormente. Vale recalcar que corresponden únicamente a los creados por la autora, los demás documentos que soportan la implementación de algunos controles ya son manejados por la DTI a través del Sistema de Gestión de Calidad (Ver Anexo 21).

Los documentos que tienen el código de calidad para el SGC (Sistema de Gestión de Calidad) y se deben subir a portal tienen su aprobación por la Dirección de Tecnología Informática.

La codificación se realiza así:
Tipo de documento – Proceso – Número del consecutivo + Nombre del documento

Tabla 28. Identificación de documentos

Tipo documento		**Proceso**	
Registro	R	Tecnología informática	TI
Instructivo	I	Help Desk	HD
Política	PL	Diseño y Desarrollo	DD
Procedimiento	P	Administración de Proyectos	AP
Anexo	A		

Fuente: Autora

6.2.2. Requisitos de la ISO 27001:2005

Teniendo en cuenta los requerimientos de la norma, se levantó un registro donde se encuentra la documentación mínima exigida por la misma. Se verifica la existencia de cada documento en la Dirección de Tecnología Informática (Ver Anexo 20).

7. RESULTADOS

Desde el mes de Junio de 2011, la Dirección de Tecnología Informática comenzó a trabajar en el estudio, análisis, adecuación y gestión de las actividades necesarias para implementar un SGSI a la luz de la norma ISO 27001:2005, en la búsqueda de una futura certificación.

Esta norma abarca todo lo relacionado con la seguridad de la información, y su objetivo principal es proteger la información sensible y establecer los puntos de referencia para cumplir con los requisitos legales en cuanto a protección de datos se refiere.

La formulación y cumplimiento de los objetivos específicos de este proyecto, se basaron en las actividades de ingeniería realizadas y dieron paso a un gran avance en la DTI. En este capítulo se evidencian y condensan los resultados obtenidos.

7.1. RESULTADOS POR FASES

La Tabla 29 muestra los resultados generados en base a los requerimientos de la norma.

Tabla 29. Resultados y avances proceso implantación SGSI - ISO 27001

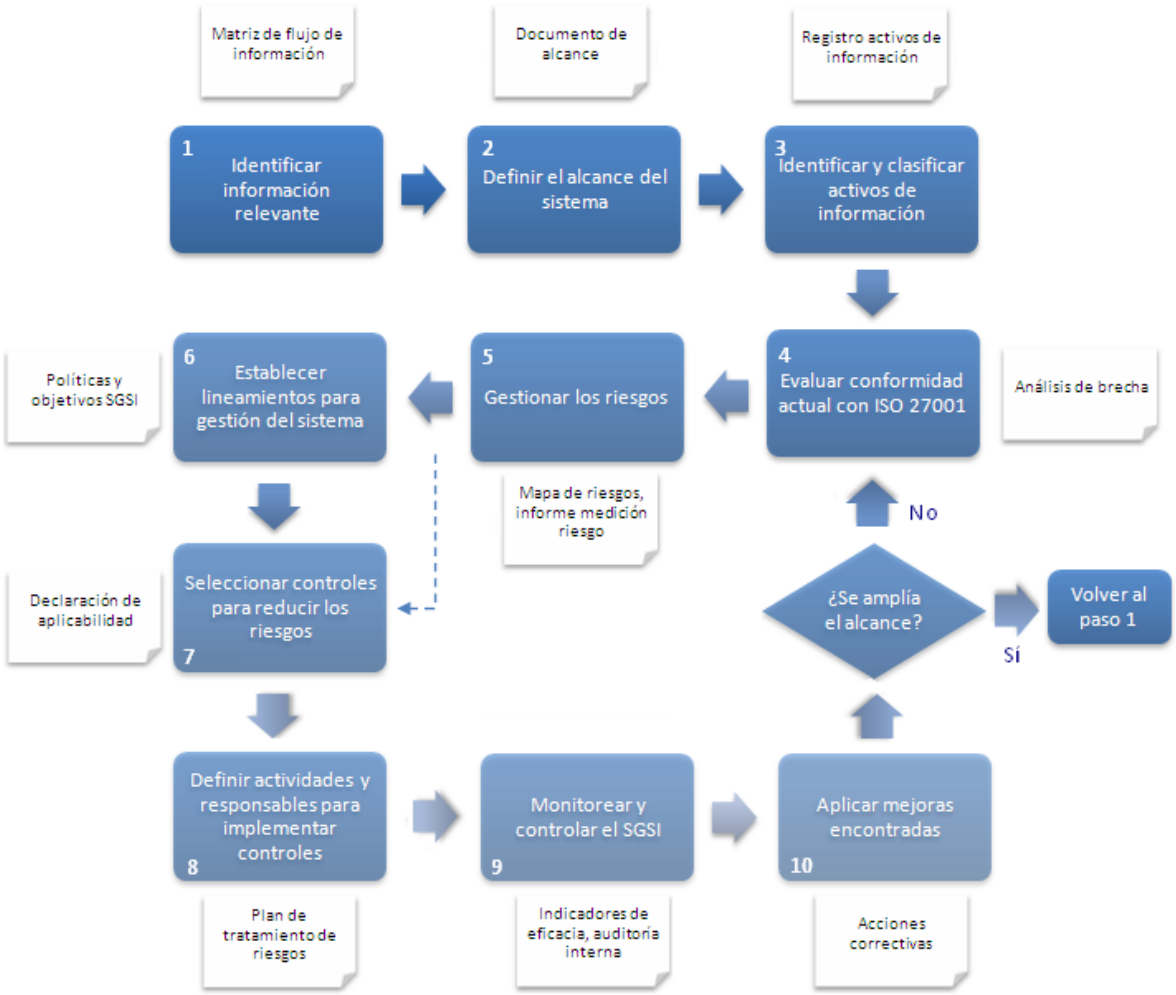
				Actividad	Resultado	Estado
PLANIFICAR	**Fase 1:** Análisis de la situación actual de la seguridad de información	Planificar	Definición responsabilidades, elaboración cronograma, seguimiento (reuniones), recursos, tiempos.	Identificar información relevante	Matriz flujo de información UEN	Completo
				Elaborar inventario de activos de información	Registro activos de información FCV	Completo
		Gestionar	Obtener aprobación de la Dirección y tener en cuenta los objetivos estratégicos. Determinar el estado en el que se encuentra la DTI respecto a la seguridad de información	Definir alcance del sistema	Alcance del SGSI (para DTI)	Completo
				Verificar los controles de la norma actualmente implementados y su nivel	Análisis de brecha	Completo
	Fase 2: Análisis y Gestión de Riesgos	Analizar	Identificar los riesgos más importantes y analizar los riesgos.	Definir el enfoque de la gestión de riesgos	Metodología gestión de riesgo	Completo
				Identificar amenazas y vulnerabilidades	Matriz relación amenazas y vulnerabilidades	Completo
		Evaluar	Valorar y calcular los riesgos	Determinar los valores críticos de integridad, disponibilidad y confidencialidad	Tasación de activos de información (en Mapa de Riesgos)	Completo
				Calcular impacto y probabilidad de ocurrencia del riesgo	Mapa de Riesgos	Completo
				Definir y seleccionar las opciones de tratamiento de riesgo		Completo
				Evidenciar los resultados	Informe medición de riesgo	Completo
	Fase 3: Establecimiento del SGSI	Divulgación	Estructurar los procedimientos de gestión del SGSI y sensibilizar al personal.	Definir política y objetivos de seguridad	Manual de políticas de calidad y seguridad de información (modificadas). Objetivos del SGSI	Completo

				Seleccionar los controles aplicables para la DTI	Declaración de aplicabilidad	Completo
				Recopilar documentos de seguridad	Documentos de seguridad actuales en la DTI	Completo
				Estructurar procedimientos de gestión del SGSI	Documentos (procedimientos, instructivos, registros) de gestión del SGSI	Completo
HACER	**Fase 4:** Implantación del SGSI	Implementar	Impartir planes de formación y concientización, crear documentación soporte a los controles. Implantar políticas.	Elaboración e implementación del plan de tratamiento de riesgos	Plan de tratamiento de riesgos (PTR)	Completo
				Crear e impartir planes de formación y concientización	Planes de formación y concientización	Faltó impartir planes: por la necesidad de capacitaciones
				Implantar los controles seleccionados y descritos en el PTR	Documentos creados de la DTI	Faltaron algunos controles: se requería inversión o tiempo mayor a 3 meses
VERIFICAR	**Fase 5:** Control y revisión del SGSI	Control	Detectar los errores en los resultados de la gestión de riesgos. Identificar eventos de seguridad.	Detectar errores en la implementación	--	Se corrigieron errores detectados en el proceso. Debe hacerse seguimiento continuo
				Establecer métricas de seguridad	Revisión del cumplimiento de los objetivos de los controles	Recomendable: utilizar métricas de la ISO 27004
		Revisión	Realizar auditorías internas del SGSI. Revisiones por parte de la Dirección.	Realizar auditorías internas	--	Se requieren auditores especializados. Falta aprobación de pre auditoría con el ICONTEC
ACTUAR	**Fase 6:** Mantenimiento y mejora del SGSI	Seguimiento	Asegurar la continuidad de las actividades, apoyar al personal en el proceso.	Establecer acciones de mejora	--	No se ha completado la fase debido a que se cumplió la fase 4 y se está a espera de la aprobación de la pre auditoría con el ICONTEC
				Ejecutar acciones preventivas, correctivas y de mejora		
		Mejora	Implementar acciones de mejora.	Implantar mejoras al SGSI		

Fuente: Autora

En la siguiente figura se muestra un modelo general del proceso de implementación del SGSI en la Dirección de Tecnología Informática de la FCV.

Figura 18. Modelo del proceso de implementación del SGSI



Fuente: Autora

7.1.1. Evidencias de los controles implementados (documentación)

En el Anexo 21 se encuentra el registro de la documentación realizada.

7.2. APORTES A LA DTI Y A LA EMPRESA

- Se llevaron a cabo una serie de actividades y documentos que dieron soporte oportuno a los objetivos estratégicos de la DTI. Por medio de cada una de las fases, se iba haciendo evidente la necesidad de gestionar adecuadamente los activos de información, por cuanto se realizó un diagnóstico de lo que se necesita para alcanzar la conformidad con la ISO 27001:2005.

- El resultado del presente proyecto de grado tuvo tan buena acogida e impacto al interior de la DTI que, se propuso y se aspira obtener la certificación con la ISO 27001:2005 para este año 2012; ya que el diagnóstico y las actividades realizadas permitieron dar un empuje a la propuesta brindada por la práctica empresarial, y dieron paso a un mayor nivel de conformidad a los requisitos de la norma, lo cual facilita y materializa este objetivo estratégico de la DTI para contar con el certificado de tan notable estándar.

- Los resultados obtenidos en la fase 4, se compartieron al Comité de Seguridad de Información y a la Dirección Ejecutiva, con el fin de contar con la autorización y apoyo tanto de ellos como de la Oficina de Planeación y Calidad; ya que es importante generar una cultura de seguridad a nivel organizacional y que estos lineamientos se conozcan no sólo al interior de DTI sino de toda la empresa.

7.2.1. Hallazgos

- En un principio, el objetivo de contar con el apoyo de la practicante era llevar a cabo un diagnóstico de la conformidad con la ISO 27001:2005 para toda la entidad. Habiéndose identificado la información relevante para cada UEN por medio de la matriz de flujo de información, además de haber visualizado la interacción de los procesos de cada UEN y Direcciones por medio de los diagramas de elipses (presentado en el Anexo 10 el de DTI); se observó y

concluyó que debido a la magnitud de la empresa, por el momento no era posible determinar un alcance global.

- La DTI está encargada de la custodia de la información manejada y procesada por los sistemas de la FCV, así como de sus clientes y proveedores. Por esta razón, es la Dirección que se responsabilizó por preceder la implementación de un SGSI al interior de la empresa, buscando crear un modelo duplicable para las demás UEN y Direcciones.

- Se encontró una evidente necesidad por organizar los procesos y el flujo de información entre ellos, ya que debido al constante crecimiento de la FCV, se maneja cada vez más volumen de información. Esto debe ser tratado con cuidado, pues la legislación avanza conforme la información se convierte en más que un activo de las empresas.

- Para poder continuar con el proceso, es necesario realizar una pre-auditoria con el ICONTEC, de esta forma se revisaría la situación actual de conformidad al ente certificador, y conocer exactamente los puntos que según esta entidad requieren un tratamiento oportuno en cuanto a seguridad de la información.

7.2.2. ¿Por qué continuar con el proceso de implementación?

Los aportes de la práctica empresarial no sólo se evidencian en el propósito de la DTI de lograr la certificación, sino también de la gestión que se está llevando a cabo actualmente para continuar con el proceso; y así como se presentó a la Dirección Ejecutiva sobre su importancia, en este documento se mostrarán dichas razones:

1. Se disminuiría la cantidad de procesos legales por pérdida de información al ser resguardada de manera adecuada, ya que se tiene una responsabilidad por la

custodia de la información al ser una clínica (Historia Clínica Electrónica). Debido a esto, es obligatorio el cumplimiento de diversas leyes, resoluciones y decretos sobre protección de datos privados, derechos de autor y Habeas Data; lo cual debe ser soportado por un SGSI, que brinda las bases y organización de los procesos de la empresa para cumplir con todas las obligaciones que le conciernen.

2. Es un modelo que no sólo se puede adoptar al interior de la DTI, sino que también puede implantarse en cada una de las UEN y Direcciones de la FCV, teniendo en cuenta el constante crecimiento de la organización (Convenios con hospitales internacionales, construcción de la zona franca mixta, entre otros).

3. Ventaja competitiva en desarrollo y comercialización de software. La FCV cuenta con su propia fábrica de software, contar con la certificación ISO 27001:2005, no sólo brinda confiabilidad a sus clientes, sino que también es un aspecto que demuestra excelencia en los servicios y productos.

4. Garantizar el cumplimiento a las autoridades competentes de los aspectos legales aplicables.

RECOMENDACIONES

Conformar un equipo de seguridad de información que lleve a cabo seguimiento y control al proceso, esté pendiente de aplicar mejoras y busque siempre estar actualizado y al tanto de los requisitos de la norma. Este equipo debería estar conformado mínimo por el personal descrito en la sección 4.3; que incluyen un líder, un ingeniero de sistemas soporte y un analista de seguridad de información, bajo el apoyo del Comité de Seguridad de Información.

A medida que se avanza en el proceso de implementación y se obtienen resultados positivos y satisfactorios, se podría ampliar el alcance del sistema. Se requiere para ello conocer las necesidades de la Dirección interesada, establecer un compromiso y ajustar el plan de implementación utilizado en la DTI para los nuevos procesos.

Se debe buscar la forma de integrar varios procedimientos, instructivos y registros, de manera que haya un nivel de cohesión entre las actividades, los procesos y los documentos, y se disminuye entonces la saturación de documentación. Esto se deduce al recordar que la norma no exige un documento por cada control implementado, entre más sencillez haya en el desarrollo de las actividades para la implementación del sistema y su documentación, mejor.

Se debe llevar a cabo la gestión de riesgos nuevamente, cuando el sistema esté funcionando adecuadamente con referencia a los objetivos establecidos, y comparar los resultados con los obtenidos en esta etapa de pre certificación. De esta manera se puede analizar qué tanto se ha logrado con la implantación del SGSI y qué tan eficaz ha sido el proceso.

La FCV es una organización de constante crecimiento y cambio, por lo tanto es muy importante estandarizar las actividades de negocio y saber cómo gestionar la información. Más aún en la existencia del proyecto zona franca Hospital Internacional, el emprendimiento de la implementación de un SGSI en la empresa se debe hacer en este momento oportuno.

A partir del desarrollo de este Trabajo de Grado se pueden derivar proyectos de gran aplicabilidad para la Ingeniería de Sistemas. No sólo en el campo de la seguridad informática, que poco a poco ha tomado auge; sino también desde el punto de vista de la ingeniería del software, pues la sistematización computacional para el proceso de implementación, documentación y seguimiento, sería una excelente herramienta de apoyo.

Ya que en un SGSI el sujeto es la información, la labor y campo de acción de un Ingeniero de Sistemas llega a ser de gran importancia, ya que sus conocimientos en tecnologías y sistemas de información brindan apoyo no sólo a la seguridad de información, sino también a la seguridad informática, lo cual complementa todos los aspectos de un SGSI. Esto puede marcar la diferencia en el éxito del proceso de implementación.

El campo de acción para este enfoque de la Ingeniería de Sistemas, para aquellos estudiantes que desearan realizar su proyecto de grado por medio de la práctica empresarial, cada vez está tomando más fuerza en las empresas. Se requiere emprendimiento por parte de los estudiantes de la EISI y futuros egresados, ya que los conocimientos obtenidos en la carrera permiten una visión más global del SGSI y su implementación. Esto se puede materializar por medio de un convenio entre las instituciones, pues actualmente la FCV requiere de apoyo continuo en su búsqueda por la certificación con la ISO 27001:2005, proporcionando oportunidades y experiencia para el desarrollo del Ingeniero de Sistemas en el ámbito de seguridad de información.

CONCLUSIONES

La creación del plan de implementación de la ISO 27001:2005 en la FCV a través de práctica empresarial, se había proyectado hacia toda la institución en un principio, pero al conocer su gran tamaño se tuvo que aterrizar en la DTI, quien sería el modelo de réplica para las demás UEN. Por tanto es necesario demostrar a la Dirección Ejecutiva que la implementación de un SGSI es una inversión más que un gasto, pues de esto depende el avance de la certificación en toda la FCV.

Esta experiencia permitió a la autora conocer otros aspectos de la Ingeniería de Sistemas, el campo de aplicación de la seguridad de información puede ser de gran incumbencia para estos profesionales, ya que a diferencia de otros sistemas de gestión, en el SGSI el sujeto es la información; y en esta materia los Ingenieros de Sistemas cuentan con los conocimientos apropiados.

Se logró que al interior del Departamento de Tecnología Informática, los jefes de área y responsables por los activos de información utilizaran las herramientas brindadas por la norma para gestionar sus actividades orientadas a la seguridad de información.

Además, se logró el reconocimiento por parte del Director de DTI de la importancia de la implementación de la norma, por el hecho de brindar la ventaja competitiva, el cumplimiento legal, la disminución de gastos y conocimiento propio; tanto así que se presentó como un proyecto a desarrollar en el 2012 a la Junta Directiva, para el apoyo y aprobación por parte de la Dirección Ejecutiva.

La gestión de la seguridad de información no es un tema desconocido en el país, pero sí es un asunto incipiente (y difícil de promover) en la mayoría de empresas que necesita de un impulso para lograr conocer y obtener sus beneficios.

Las organizaciones pueden integrar la ISO 27001:2005 con otras normas y sistemas de gestión, en el caso de la FCV y la ISO 9001:2008 esto fue de gran apoyo; pues contar con un SGC facilita el proceso, ya que existe un nivel de correspondencia entre ellas.

Determinar el alcance del sistema es fundamental. Es muy recomendable definir inicialmente un alcance reducido que permita un seguimiento controlable y no lleve al fracaso inmediato, principalmente por dos razones: la FCV es una empresa de gran tamaño y el SGSI es un tema relativamente nuevo dentro de la organización.

Es necesario adoptar una metodología de implementación que se ajuste a las necesidades y disponibilidades de la organización, en materia de tiempo, recursos, personal y dedicación. Conocer los procesos de negocio, el desempeño organizacional, tener metas claras y voluntad real para alcanzarlas, son factores claves en un proyecto de implementación exitosa y provechosa de un SGSI.

Las empresas tienen la posibilidad de integrar su información y estandarizar sus procesos, gestionando la seguridad de información. De esta manera se protege la información y se asegura más la continuidad del negocio. Especialmente para organizaciones en proceso de continuo crecimiento, es importante el cumplimiento de los estándares existentes para los SGSI.

Luego de este proceso, y en base a las mejoras que se deban implementar, se puede comenzar el proceso de certificación, el cual cuenta con acompañamiento de profesionales en el campo, auditorías y posteriormente aprobación de certificación, convirtiéndose así en la primera entidad del sector salud en conseguir este gran logro.

BIBLIOGRAFÍA

ALEXANDER, Alberto G. Diseño de un Sistema de Gestión de Seguridad de Información : Óptica ISO 27001:2005. Primera edición. Bogotá D.C. : Alfaomega Colombiana S.A., 2007. 176 p.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION. International Standard ISO/IEC 27005:2008. Primera edición 2008/06/15. [Consultado 12 de Agosto 2011]. Disponible en físico en servidor de la FCV.

OSSA PARRA, Marcela (Comp.). Cartilla de citas : Pautas para citar textos y hacer listas de referencias. Bogotá: Universidad de Los Andes, Decanatura de Estudiantes, 2006. 90p.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Estándar Internacional ISO/IEC 27001 en español. [En línea]. Primera edición 2005/10/15. [Consultado 2 de Mayo]. Disponible en <http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf>

ISO 27000. Certificación, SGSI. En: El portal de ISO 27001 en español. [En línea]. [Consultado 9 de Mayo 2011]. Disponible en <http://www.iso27000.es/index.html>

ATSEC. The information security provider. ISMS Implementation Guide. [En línea]. [Consultado 20 Julio 2011]. Disponible en <http://www.atsec.com/downloads/documents/ISMS-Implementation-Guide-and-Examples.pdf>

Análisis y Modelado de Amenazas. [En línea]. [Consultado 21 julio 2011]. Disponible en <http://metal.hacktimes.com/files/Analisis-y-Modelado-de-Amenazas.pdf>

Gestión de Riesgo en la Seguridad Informática, Wordpress. Matriz para el análisis de riesgo. [En línea]. [Consultado 22 de Julio 2011]. Disponible en <http://protejete.wordpress.com/gdr_principal/matriz_riesgo/>

Seguridad de la Información en Colombia (ISO 27000). Marco legal de Seguridad de la Información en Colombia. [En línea]. [Consultado 25 de Julio 2011]. Disponible en <http://seguridadinformacioncolombia.blogspot.com/search/label/Leyes>

SEHINE, Seguridad Informática y Hacking Ético. En: Definición del alcance del SGSI en la norma ISO 27001. [En línea]. [Consultado 27 Julio 2011]. Disponible en <http://www.seinhe.com/posts/16-definicion-del-alcance-del-sgsi-en-la-norma-iso-27001>

ArCERT Argentina, Coordinación de emergencias en Redes Teleinformáticas. En: política, principales amenazas. [En línea]. [Consultado 10 de Agosto 2011]. Disponible en<http://www.arcert.gov.ar/politica/versionimpresa.htm>

KOSUTIC, Dejan. ISO 27001 & BS 25999 [En línea]. Blog. [Consultado 10 de Agosto 2011]. Disponible en <http://blog.iso27001standard.com/es/>

El proceso de gestión de riesgos. [En línea]. [Consultado 2 de Septiembre 2011]. Disponible en <http://www.aduana.cl/prontus_aduana/site/artic/20070228/asocfile/20070228130834/asocfile120050916161822.pdf>

Departamento Administrativo de la Función Pública. Guía Administración del Riesgo. [En línea]. [Consultado 2 de Septiembre 2011]. Disponible en <http://200.26.134.109:8092/unisucre/hermesoft/portal/home_1/rec/arc_2129.pdf>

Segu - info, seguridad de información. En: artículos. [En línea]. [Consultado 6 de Septiembre 2011 Disponible en<http://www.segu-info.com.ar/articulos/59-escribiendo-politicas-seguridad.htm>

ANÁLISIS DE RIESGOS. Gestión de Riesgos / Tratamiento. [En línea]. [Consultado 29 de Septiembre 2011]. Disponible en <http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/5TratamientodelRiesgo(AR)_es.pdf>

Seguridad y Gestión, Planes de Tratamiento de Riesgo. Blog. [En línea]. [Consultado 29 de Septiembre 2011]. Disponible en <http://secugest.blogspot.com/2006/11/planes-de-tratamiento-de-riesgos.html>

BRIGHT HUB. Creating a Risk Management Plan. [En línea]. [Consultado 5 de Octubre 2011]. Disponible en <http://www.brighthub.com/office/project-management/articles/31710.aspx>

INTEROPERABILITY MONTANA. Risk Management Plan. [En línea]. [Consultado 7 de Octubre 2011]. Disponible en <http://www.saudipmc.com/eng/veikko-pdf/RMPlan.pdf>

ICONTEC. Norma Técnica Colombiana NTC 1486, Presentación de tesis, trabajos de grado y otros trabajos de investigación. [En línea]. [Consultado 12 Enero de 2012]. Disponible en <http://palmira.univalle.edu.co/la_sede/dependencias/biblioteca/Documentos/NormasTrabajosDeGrado-2010.pdf>

ANEXOS

Nota: Los anexos de este Proyecto de Grado se encuentran en la carpeta “ANEXOS” en el archivo Anexos.doc dentro de este CD, debido a su extensión. La información contenida en los formatos, listas de chequeo, tablas, registros y gráficas es de propiedad de la Fundación Cardiovascular de Colombia. Algunos datos fueron modificados, reservados o excluidos para la presentación de este documento (principalmente en los Anexos), de conformidad a las políticas de seguridad de información de la empresa.