PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA ENTIDAD ESTATAL DE SALUD DE ACUERDO A LA ISO/IEC 27001:2013

Tesis para optar por el Título de Ingeniero Informático, que presenta el bachiller:

Vasco Rodrigo Talavera Álvarez

ASESOR: Mg. Moisés Villena Aguilar

Lima, Mayo del 2015

RESUMEN

En la actualidad los sistemas que se utilizan para almacenar, procesar y transmitir información se encuentran en toda clase de instituciones de diferentes rubros y funciones. Los sistemas de información se han vuelto más complejos debido a la globalización que tiene por consecuencia que las distancias geográficas ya no supongan un obstáculo.

De esta forma se tiene que existe una cantidad cada vez mayor de personas que tienen acceso a información que podría ser crítica para las diferentes empresas e instituciones en las que trabajan. Adicionalmente a este riesgo interno, siempre se tiene presente el riesgo que supone la fuga de información sensible ya sea por medio de personas que cuentan con acceso a dicha información, como por terceros que han accedido a ella mediante algún mecanismo de ataque.

En respuesta a este nuevo escenario, las instituciones públicas han sido llamadas a realizar la implementación de diversos controles a través de un Sistema de Gestión de Seguridad de la Información – a través de diferentes normas, entre ellas la Norma Técnica NTP ISO/IEC 27001 – con la finalidad de asegurar el buen uso y protección de la información crítica que manejen, ya sea de clientes o información estratégica interna.

El presente trabajo de fin de carrera desarrolla el Análisis y Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad pública del sector Salud – el Instituto Nacional Materno Perinatal – sujeta al cumplimiento de la normativa vigente relativa a Seguridad de la Información.

DEDICATORIA

A Dios y María Auxiliadora, por regalarme la vida y poner a las personas indicadas en mi camino siempre.

A mis padres Rosaura y Hugo, por todo su apoyo al escuchar mis dudas, sus consejos al afrontar las dificultades y su paciencia al oírme hablar tantas veces sobre este proyecto.

A mis hermanas Adriana y Ana Lucía, por apoyarme durante el desarrollo de este proyecto, sobre todo en la preparación de la defensa del mismo.

A mi amada Fátima, mi compañera inseparable, por ser mi apoyo, mi inspiración y por estar siempre a mi lado. Por escucharme, preguntarme, corregirme, darme ánimos y compartir conmigo la experiencia de desarrollar en su compañía el presente trabajo de fin de carrera y su tesis hermana.

AGRADECIMIENTOS

Al Mg. Moises Villena, por el tiempo brindado, la experiencia compartida y los consejos, y los conocimientos impartidos en las aulas de clase, pilares sobre los cuales logré alcanzar la meta de finalizar este proyecto.

Al Dr. Manuel Tupia, a quien admiro y considero un modelo de docente y profesional a seguir, espero que su vocación, el cual llega más allá de las clases, se mantenga siempre.

Al Ing. Nancy Alvarado y al Ing. Joseph Ramírez, por la oportunidad y conocimientos compartidos para el desarrollo del presente proyecto.

A Johanna Cuba por confiar en mí y abrirme las puertas al mundo de la Seguridad de la Información junto con Mónica Ghersi, Giovanna Pizarro, Cynthia Herrera, Diego Rodríguez, Henry Zapata y Arturo Cruz a quienes debo mucho del conocimiento que puse en práctica en el desarrollo de este proyecto.

Tabla de contenido

1 CAPÍTULO 1: GENERALIDADES 10

1.1 PROBLEMÁTICA 10
1.2 OBJETIVO GENERAL 13
1.3 OBJETIVOS ESPECÍFICOS 13
1.4 RESULTADOS ESPERADOS 13
1.5 HERRAMIENTAS, MÉTODOS Y PROCEDIMIENTOS 13
1.5.1 MAPEO 14
1.5.2 NORMA ISO/IEC 27001:2013 14
1.5.3 BUSINESS PROCESS MANAGEMENT (BPM 2.0) 16
1.5.4 NORMA ISO/IEC 31000:2009 16
1.5.5 NORMA ISO/IEC 27002:2013 17
1.5.6 NORMA ISO/IEC 27799:2008 18
1.6 ALCANCE 18
1.7 LIMITACIONES 19
1.8 RIESGOS DEL PROYECTO 20
1.9 JUSTIFICACIÓN Y VIABILIDAD 21
1.9.1 JUSTIFICATIVA DEL PROYECTO DE TESIS 21
1.9.2 ANÁLISIS DE VIABILIDAD DEL PROYECTO DE TESIS 22
1.10 CRONOGRAMA DE DESARROLLO DEL PROYECTO 23

2 CAPÍTULO 2: MARCO TEÓRICO Y ESTADO DEL ARTE 24

2.1 MARCO TEÓRICO 24
2.1.1 MARCO CONCEPTUAL 24
2.1.2 MARCO REGULATORIO / LEGAL 37
2.2 ESTADO DEL ARTE 46
2.2.1 FORMAS EXACTAS DE RESOLVER EL PROBLEMA 47
2.2.2 FORMAS APROXIMADAS DE RESOLVER EL PROBLEMA 51
2.2.3 CONCLUSIONES SOBRE EL ESTADO DEL ARTE 56

3 CAPÍTULO 3: DOCUMENTACIÓN EXIGIDA POR LA NORMA ISO/IEC 27001:2013 57

3.1 CASO DE NEGOCIO 57
3.1.1 NECESIDADES DEL NEGOCIO Y DESCRIPCIÓN DEL PROYECTO 58
3.2 ALCANCE DEL SGSI 63
3.3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 66

4 CAPÍTULO 4: MAPA DE PROCESOS DEL ALCANCE 68

4.1 MODELADO DE LOS PROCESOS DE NEGOCIO ESTABLECIDOS EN EL ALCANCE DEL PROYECTO 68

5 CAPÍTULO 5: METODOLOGÍA DE ANÁLISIS DE RIESGOS 72

6 CAPÍTULO 6: METODOLOGÍA DE VALORACIÓN DE ACTIVOS 75

7 CAPÍTULO 7: MAPA DE RIESGOS 80

7.1 INVENTARIO DE ACTIVOS 80
7.2 IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS 81

8 CAPÍTULO 8: DECLARACIÓN DE APLICABILIDAD 82

9 CAPÍTULO 9: CONCLUSIONES Y RECOMENDACIONES 83

9.1 OBSERVACIONES 83
9.2 CONCLUSIONES 85
9.3 RECOMENDACIONES Y TRABAJOS FUTUROS 87

REFERENCIAS BIBLIOGRÁFICAS 90

Índice de Tablas

Tabla 1 Mapeo de Herramientas a utilizar por Resultado esperado 14

Tabla 2 Riesgos identificados del proyecto 20

Tabla 3 Criterios de probabilidad utilizados en el proyecto 73

Tabla 4 Criterios de impacto utilizados en el proyecto 73

Tabla 5 Matriz de calor utilizado para la valoración de riesgos identificados en el proyecto.....74

Tabla 6 Modelo de Matriz de inventario de Activos de Información.....78

Tabla 7 Escala de valoración de Activos de Información 79

Índice de Ilustraciones

Ilustración 1 Cronograma de desarrollo del proyecto 23

Ilustración 2 Estrategia de mejora continua del SGSI, Ciclo de Deming 42

Ilustración 3 Cronograma establecido para la implementación del SGSI para las instituciones normadas por la NTP-ISO/IEC 27001:2008.....59

Ilustración 4 Funciones del Servicio de Admisión y Consultorios Externos 64

Ilustración 5 Proceso de negocio de Admisión de Pacientes 70

Ilustración 6 Proceso de negocio de Emisión de Copia de Historia Clínica 71

1 CAPÍTULO 1: Generalidades

1.1 Problemática

En la actualidad los sistemas que se utilizan para almacenar, procesar y transmitir información se encuentran en toda clase de instituciones de diferentes rubros y funciones. Los sistemas de información se han vuelto más complejos debido a la globalización que tiene por consecuencia que las distancias geográficas ya no supongan un obstáculo. De esta forma se tiene que existe una cantidad cada vez mayor de personas que tienen acceso a información que podría ser crítica para las diferentes empresas e instituciones en las que trabajan. Adicionalmente a este riesgo interno, siempre se tiene presente el riesgo que supone la fuga de información sensible ya sea por medio de personas que cuentan con acceso a dicha información, como por terceros que han accedido a ella mediante algún mecanismo de ataque.

El Instituto Nacional Materno Perinatal – INMP (ex Maternidad de Lima) es una entidad que pertenece al sector público especializada en brindar servicios de salud a mujeres gestantes y neonatos. Como entidad prestadora de salud maneja información sobre sus pacientes que permite mantener un historial de las atenciones y diagnósticos de los mismos – contenido en la Historia Clínica que es el principal documento utilizado por la institución – pero que además contiene información personal que identifican al paciente y debe ser protegida ya sea para poder garantizar la correcta atención de los pacientes como para evitar la fuga de información que pueda ser utilizada de manera maliciosa por alguna persona o institución externa al flujo de información.

Como entidad pública el INMP se encuentra sujeto a las regulaciones establecidas por el estado en diferentes aspectos relacionados con las actividades que realiza, entre ellos tenemos la Ley de Protección de Datos

Personales. Dicha norma establece directivas a seguir para la identificación de información personal y sensible, así como las consideraciones que las instituciones que utilizan este tipo de información deben tener en cuenta durante el manejo de la información de sus clientes.

Si bien se cuenta con una serie de normas estándar internacionales, publicadas por la Organización Internacional de Normalización (ISO), en el Perú se han definido leyes alineadas a éstos para que puedan ser aplicadas al contexto de las empresas existentes en el país en cuanto a la gestión de la información utilizada por las instituciones públicas.

Estas iniciativas tuvieron su inicio en el año 2006 con la publicación del documento “Lineamientos de Política de Seguridad de la Información del Ministerio de Salud” (MINSA, 2006), la cual se aplica a dicha institución gubernamental y sus dependencias en vista de la importancia de la información que se maneja en dicho sector. Dos años más tarde se aprobó la Norma Técnica Peruana (NTP) ISO/IEC 27001:2008 (CNB - INDECOPI, 2008) la cual adquirió carácter de obligatoria en el mes de mayo del 2012 teniendo por objetivo todas las organizaciones públicas del país.

Esta norma técnica exige que las entidades públicas realicen la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo las recomendaciones y controles señalados en la misma, la cual no detalla específicamente la manera en la que éste sistema de gestión debe ser implementado ya que sus recomendaciones son generales, teniendo dichas instituciones que realizar las diferentes fases detalladas en el plan de Implementación Incremental publicada por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI).

Adicionalmente, la aprobación de la nueva Ley 29733 sobre Protección de Datos Personales implica un frente adicional que las instituciones públicas deben cubrir en cuanto al manejo de la información de sus usuarios.

Analizando el escenario actual, se puede apreciar que el INMP como parte de las instituciones públicas debe adaptarse a los nuevos cambios legislativos mediante la implementación, de manera complementaria con las nuevas normas que regulan los temas de privacidad y seguridad, de mecanismos de

control y seguimiento de seguridad de la información. Sin embargo, como se mencionó previamente, la normativa aprobada si bien da recomendaciones a seguir para la Implementación de un SGSI, no indica exactamente la metodología o pasos a seguir para lograr este objetivo.

La necesidad de las instituciones públicas de contar con un análisis que les permita realizar el diseño de un SGSI, en conjunto con los controles correspondientes al mismo como respuesta a la exigencia legal establecida por las normas previamente mencionadas, además de la falta de una guía que acompañe el proceso a seguir para realizar dicho diseño a medida según los requerimientos específicos de una entidad prestadora de salud como el INMP, constituyen la problemática que este Proyecto de Fin de Carrera pretende resolver siguiendo las buenas prácticas y estándares internacionales correspondientes que permitan realizar una identificación de la información crítica con la que trabaja la institución y en consecuencia definir los riesgos a los que se encuentra expuesta y los controles que deberían implementarse para garantizar su seguridad.

1.2 Objetivo general

Diseñar un sistema de gestión de seguridad de la información para una institución estatal de salud, de acuerdo a la norma ISO/IEC 27001:2013.

1.3 Objetivos específicos

Los objetivos específicos que tiene el presente proyecto son los siguientes:

1. Elaborar la documentación exigida por la norma ISO 27001.
2. Realizar el modelado de los procesos correspondientes al alcance del Sistema de Gestión de Seguridad de la Información.
3. Elaborar una metodología de análisis de riesgos y valoración de activos.
4. Elaborar el mapa de riesgos de los procesos del alcance.
5. Elaborar la declaración de aplicabilidad.

1.4 Resultados esperados

Los resultados esperados correspondientes a los objetivos específicos planteados son los siguientes:

- Resultado 1 para el objetivo 1: Documentación exigida por la norma ISO/IEC 27001.
- Resultado 2 para el objetivo 2: Mapa de procesos del alcance.
- Resultado 3 para el objetivo 3: Metodología de análisis de riesgos.
- Resultado 4 para el objetivo 3: Metodología de valoración de activos.
- Resultado 5 para el objetivo 4: Mapa de riesgos.
- Resultado 6 para el objetivo 5: Declaración de aplicabilidad.

1.5 Herramientas, métodos y procedimientos

A continuación, se procederá a detallar las herramientas y metodologías que serán utilizadas durante el desarrollo del presente proyecto, con la finalidad de alcanzar los diferentes objetivos establecidos para el mismo.

1.5.1 Mapeo

Resultado esperado	Herramienta a utilizar
RE1: Documentación exigida por la norma ISO 27001	**Norma ISO 27001** estándar internacional que especifica los requisitos a cumplir para establecer un SGSI.
RE2: Mapa de procesos del alcance	**Business Process Management (BPM 2.0)** metodología que agrupa varias herramientas cuya finalidad es el análisis y control de los procesos de negocio de una empresa.
RE3: Metodología de análisis de riesgos	**Norma ISO 31000** estándar internacional que sirve como referencia a la valuación y gestión de riesgos.
RE4: Metodología de valoración de activos	
RE5: Mapa de riesgos	
RE6: Declaración de aplicabilidad	**Norma ISO 27002** conjunto de objetivos de control y controles que pueden ser aplicados para el tratamiento del riesgo. **Norma ISO 27799** norma que aplica los conceptos contenidos en la norma 27002 al entorno de las instituciones de salud.

Tabla 1 Mapeo de Herramientas a utilizar por Resultado esperado Fuente: Elaboración propia

1.5.2 Norma ISO/IEC 27001:2013

Estándar internacional desarrollado como una guía para el análisis, implementación, control y mantenimiento de un Sistema de Gestión de Seguridad de la Información, a través del establecimiento de un grupo de requisitos a cumplir con este motivo. Dado su enfoque orientado a los procesos de negocio, es una norma general aplicable a una gran gama de empresas, adaptándose a los diferentes giros de negocio y activos de información que éstas puedan tener. La versión correspondiente al año 2013 presenta una nueva estructura según el estándar definido por ISO/IEC para todas las normas referentes a sistemas de gestión, facilitando la integración y trabajo conjunto entre los diferentes estándares de gestión publicados por dicha entidad.

Este estándar es de uso crítico en los proyectos de análisis y diseño de SGSI's, dado que establece concretamente los pasos implicados en este proceso.

A diferencia de su versión anterior – ISO/IEC 27001:2005 – la norma actual no nombra el ciclo de Deming (Plan, Do, Check, Act) como metodología para definir el ciclo de vida – y mejora continua – del sistema de seguridad a implementar, dejando abierta la posibilidad de la entidad a elegir un modelo de mejora continua distinto y que se adapte mejor a sus necesidades. Sin embargo se utilizará el ciclo de Demming para asegurar el cumplimiento de lo requerido en la Norma Técnica Peruana NTP ISO/IEC 27001:2008 que utiliza la estructura de la norma ISO/IEC 27001:2005.

Se requiere el uso de la presente herramienta dado que la base para el proyecto de SGSI requiere que se establezca la Política de Seguridad de la Información además de servir como guía en los procesos que establezcan finalmente los siguientes ítems:

- El alcance que tendrá el SGSI sobre los procesos de la empresa.
- La política general de seguridad de la información
- La identificación y valoración de los activos de la información.
- Los riesgos a los cuales los activos identificados se encuentran expuestos.
- La selección de los controles para mitigar los riesgos que se han detectado.

Es pertinente indicar que el alcance que se ha definido para el presente estudio sólo abarca la fase de Planificación del ciclo de Deming, dado que no se pretende realizar la implantación del SGSI que se dé como resultado del mismo. (ALEXANDER, 2007) (ISO 27001, 2013) (ORMELLA, 2013)

1.5.3 Business Process Management (BPM 2.0)

El modelado de procesos es una tarea crítica y obligatoria para cualquier proyecto que pretenda establecer un Sistema de Gestión de Seguridad de la Información en alguna organización, puesto que es necesario conocer cómo se desarrollan los distintos procesos de negocio, así como el flujo de información a través de los mismos.

Esta metodología incluye diferentes herramientas – tanto de documentación, como tecnológicas – especializadas en el análisis de procesos de negocio con la finalidad de detectar oportunidades de mejora que permitan optimizarlos.

Como respuesta a la necesidad de contar con una metodología que apoye a obtener el Mapa de procesos del alcance, lo cual conlleva a que se requiera modelar los procesos de negocio críticos de la organización sobre la cual se realiza el presente trabajo, se utilizará las herramientas ofrecidas por esta metodología para la determinación del flujo de datos, actores y procedimientos que componen el alcance que se haya determinado para el alcance del proyecto.

El modelamiento de procesos se apoyará en la herramienta de modelamiento Bizagi, la cual permitirá presentar de manera gráfica el flujo de tareas que conforman los procesos de negocios que se requiera estudiar, así como la documentación que incluya los datos y conocimientos obtenidos en el levantamiento de información. (HITPASS, 2007)

1.5.4 Norma ISO/IEC 31000:2009

Estándar internacional que establece recomendaciones generales a seguir en cuanto a la gestión del riesgo sin especificar casos para algún tipo de empresa. Se basa en tres principios que conllevan a un correcto manejo de los riesgos: el primero define a la gestión del riesgo como una actividad administrativa; el segundo sugiere que la estimación de riesgos debe hacerse mediante un enfoque top-down y finalmente establece una lista no exclusiva de los posibles riesgos que pueden presentarse en una organización.

Al utilizar el ciclo de Deming (Plan, Do, Check, Act), establece los siguientes pasos generales para la implementación de un sistema de gestión de riesgos: primero establece las políticas de riesgo de la organización como soporte al proceso de gestión del riesgo en el que se realiza la identificación, análisis, valoración y manejo del riesgo. Finalmente hace un análisis de las estrategias de manejo de riesgos que se tienen actualmente y determina cuáles se deben implementar adicionalmente.

Dado el gran alcance del presente estándar, además de la complementación de la norma ISO/IEC 27001 en su última versión con el mismo, se utilizará esta norma como solución a aplicar para poder alcanzar los resultados relacionados con el estudio y gestión de riesgos en el proceso de negocio escogido para el presente proyecto. (PASSENHEIM, 2010) (GIBSON, 2010)

1.5.5 Norma ISO/IEC 27002:2013

El resultado esperado de la Declaración de Aplicabilidad será cubierto mediante el uso de la Norma ISO/IEC 27002, la cual contiene una lista de recomendaciones para la gestión de la seguridad de la información que se recomienda utilizar en la creación de este entregable. Con la ayuda de los controles generales que éste documento contiene se procede a seleccionar aquellos que aplican según el análisis previo que se ha realizado.

Específicamente en el entregable asociado se detalla los controles seleccionados para el proyecto, aquellos que ya se encuentran implementados y también aquellos que han sido excluidos. Todos los controles y objetivos de control que se detallen en este documento deben estar acompañados por la justificación correspondiente de su elección o exclusión del proyecto. (ALEXANDER: 2007) (ISO 27002, 2013) (ORMELLA, 2013)

1.5.6 Norma ISO/IEC 27799:2008

Como apoyo al último resultado esperado, se utilizará la Norma ISO 27799. Dicho documento contiene una especificación de las consideraciones que se debe tener en cuenta en el análisis y diseño de un SGSI en instituciones relacionadas al cuidado de la salud. Específicamente brinda una guía sobre la aplicación y casos especiales referentes a los controles propuestos por la norma ISO/IEC 27002. (ISO 27799, 2008)

1.6 Alcance

El presente proyecto de fin de carrera tiene por propósito generar una solución específica para una organización del sector público y específicamente del rubro salud, debido a que se tomarán los procesos institucionales de una empresa de este tipo como campo de estudio para aplicar las metodologías y herramientas anteriormente mencionadas.

El proyecto se centrará en los procesos institucionales referentes al área de admisión de pacientes, limitando el alcance que se utilice para la creación de la documentación a dos de estos procesos críticos para la operación del área indicada. El proyecto comprenderá los siguientes pasos:

- Se elaborará la Política de Seguridad de la Información correspondiente al área y proceso de negocio elegido.
- Se determinarán los activos de información críticos para el proceso de negocio escogido, así como su valoración en términos de la criticidad que éstos representan para el mismo.
- Se realizará un análisis de los riesgos presentes en la situación actual y que constituyan una posible amenaza directa o indirecta para los activos de información especificados en el análisis anterior.
- Se elaborará la documentación necesaria para establecer los controles que permitan mitigar los riesgos identificados, además de la documentación de aquellos riesgos que se decidió aceptar con su respectiva justificación.

1.7 Limitaciones

Las limitaciones para el presente proyecto de fin de carrera son las siguientes:

- Debido al tipo de proyecto y a la ventana de tiempo establecida para poder concretar este estudio, sólo se procederá con las fases de Análisis y Diseño del SGSI, dejando la implementación debido al esfuerzo y tiempo que requeriría.

Los obstáculos que podrían afectar el normal desarrollo del proyecto son los siguientes:

- Dado el alcance del estudio así como las distintas fases que comprende, podría ser necesario el acceso a ambientes en los que se encuentran activos de información críticos, lo cual podría no ser facilitado por la institución dependiendo de sus políticas internas.

1.8 Riesgos del proyecto

El desarrollo de proyectos debe tener en cuenta los riesgos a los que éstos se encuentran expuestos y que podrían ocasionar el fracaso del mismo. En el presente proyecto se han identificado los siguientes riesgos:

Riesgo identificado	Impacto en el proyecto	Medidas correctivas para mitigar
Cambio en los estándares utilizados debido a revisiones.	Impacto alto	Tener en cuenta el cronograma de nuevas publicaciones ya programadas para las normativas utilizadas.
Identificación errónea de los procesos de negocio críticos del área sobre la que se realizará el estudio.	Impacto alto	Realizar reuniones periódicas con el personal del área escogida para verificar los datos recogidos en el levantamiento de información.
Identificación errónea de los activos críticos de información y de los riesgos asociados a los mismos	Impacto alto	Realizar revisiones periódicas con el personal del área escogida y el asesor del proyecto para revisar la correcta aplicación e identificación de las metodologías escogidas.
Falta de acceso a la información necesaria para la documentación requerida por los estándares utilizados.	Impacto medio	Establecer documentos que permitan al líder de proyecto establecer una relación de confianza con la organización, que garantice el acceso a la información requerida. A pesar de la criticidad en caso se materialice este riesgo, se considera medio dadas las relaciones de confianza establecidas con el personal de la organización sobre la que se realizará el estudio
Falta de espacios de tiempo para realizar el estudio de activos y riesgos in-situ.	Impacto medio	Establecer un cronograma de visitas en las cuales se puedan realizar los procesos necesarios para el estudio de activos de información y los riesgos a los que se encuentran expuestos.

Tabla 2 Riesgos identificados del proyecto Fuente: Elaboración propia

1.9 Justificación y viabilidad

1.9.1 Justificativa del proyecto de tesis

Los resultados obtenidos a partir del presente trabajo de investigación, permitirán tener un estudio actual de los principales procesos que involucra el manejo de información crítica para el INMP – según el alcance establecido para el mismo – así como del establecimiento del análisis y diseño de un SGSI en una organización de este tipo, teniendo en cuenta el cumplimiento de las normas actuales que se apliquen a estos procesos críticos.

Dada la actual carencia de un SGSI en la organización sobre la cual se realizará el presente proyecto, además de la gran cantidad de cambios en la normativa de carácter obligatorio para las organizaciones que hagan uso de información personal y sensible en sus operaciones – por tanto el proyecto deberá alinear las políticas determinadas por el SGSI con las normas legales que no están directamente relacionadas con la seguridad de la información – suscitan la necesidad de definir pasos a seguir para la implementación de un SGSI a medida, definiéndose aquellas consideraciones especiales que se hayan integrado para cumplir los requisitos que indique la legislación vigente. De esta manera el presente proyecto servirá como un estudio que pueda servir de guía en la implementación de futuros trabajos sobre contextos similares.

La aplicación de los conocimientos adquiridos en el trabajo de fin de carrera podría influir ampliamente en la mejora de la calidad de atención a los pacientes, además de facilitar el trabajo del personal hospitalario, mediante el establecimiento de políticas que protejan la información requerida en la atención hospitalaria.

1.9.2 Análisis de viabilidad del proyecto de tesis

El actual proyecto no supone – ni contempla futuras – inversiones que se requieran como prerrequisito para la adquisición de alguna de las herramientas que se han elegido para poder alcanzar los objetivos esperados definidos. Actualmente para poder completar el proyecto, se cuenta con acceso a todas las herramientas y normas que se mencionan en el desarrollo del presente documento.

De igual manera, se ha establecido una relación de confianza entre la institución – específicamente con las áreas de Estadística e Informática y Admisión de Consultorios Externos – para la cual se está tramitando la autorización física conveniente que permita garantizar el acceso a la información necesaria para el desarrollo del proyecto de investigación.

1.10 Cronograma de desarrollo del proyecto

Dado el alcance, los objetivos y resultados esperados así como el tiempo del que se dispone para el desarrollo del presente proyecto, se ha definido el siguiente cronograma que determina las etapas a seguir.

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**Inicio del proyecto**	**63 días**	**lun 04/08/14**	**mié 29/10/14**	
2	Elección y justificación del tema	1 día	lun 04/08/14	lun 04/08/14	
3	Definición de la problemática y elaboración del marco teórico y estado del arte	8 días	mar 05/08/14	jue 14/08/14	2
4	Definición del objetivo general	1 día	vie 15/08/14	vie 15/08/14	3
5	Definición de objetivos específicos	1 día	lun 18/08/14	lun 18/08/14	4
6	Definición de resultados esperados	1 día	lun 18/08/14	lun 18/08/14	4
7	Definición del alcance y limitaciones del proyecto	1 día	mar 19/08/14	mar 19/08/14	6
8	Definición de métodos y procedimientos a utilizar	1 día	mié 20/08/14	mié 20/08/14	7
9	**Planificación del proyecto**	**3 días**	**jue 21/08/14**	**lun 25/08/14**	
10	Análisis de viabilidad y justificativa del proyecto	2 días	jue 21/08/14	vie 22/08/14	8
11	Planificación de actividades	1 día	jue 21/08/14	jue 21/08/14	8
12	Correcciones de Entregable	1 día	vie 22/08/14	vie 22/08/14	11
13	Entrega de Capitulo 1 y 2	1 día	lun 25/08/14	lun 25/08/14	12
14	Exposición de proyecto de Tesis según avance	1 día	lun 25/08/14	lun 25/08/14	12
15	**Ejecución del proyecto**	**45 días?**	**mar 26/08/14**	**lun 27/10/14**	**9**
16	Modelado de procesos críticos	9 días	mar 26/08/14	vie 05/09/14	
17	Entrega de Capitulo 3	1 día	lun 08/09/14	lun 08/09/14	16
18	Exposición de proyecto de Tesis según avance	1 día	lun 08/09/14	lun 08/09/14	16
19	Análisis de Riesgos	3 días	mar 09/09/14	jue 11/09/14	18
20	Análisis de Impacto (BIA)	3 días	vie 12/09/14	mar 16/09/14	19
21	Plan de Gestión de Crisis	3 días	mié 17/09/14	vie 19/09/14	20
22	Entrega de Capitulo 4	1 día	lun 22/09/14	lun 22/09/14	21
23	Exposición de proyecto de Tesis según avance	1 día	lun 22/09/14	lun 22/09/14	21
24	Plan de Respuesta a Emergencias	9 días	mar 23/09/14	vie 03/10/14	23
25	Entrega de Capitulo 5	1 día	lun 06/10/14	lun 06/10/14	24
26	Exposición de proyecto de Tesis según avance	1 día	lun 06/10/14	lun 06/10/14	24
27	Sustentación parcial	1 día	lun 20/10/14	lun 20/10/14	
28	Plan de recuperación de desastre	4 días	mar 07/10/14	vie 10/10/14	26
29	Planes de Continuidad de Negocios	5 días	lun 13/10/14	vie 17/10/14	28
30	Plan de Pruebas	3 días	lun 20/10/14	mié 22/10/14	29
31	Conclusiones	2 días	jue 23/10/14	vie 24/10/14	30
32	Entrega de Capitulo 6	1 día	lun 27/10/14	lun 27/10/14	31

Ilustración 1 Cronograma de desarrollo del proyecto Fuente: Elaboración propia

2 CAPÍTULO 2: Marco teórico y Estado del Arte

2.1 Marco teórico

A continuación se presentarán los principales conceptos necesarios para el completo entendimiento del desarrollo del presente proyecto, así como del Sistema de Gestión de Seguridad de la Información que se pretende alcanzar en el mismo.

2.1.1 Marco conceptual

2.1.1.1 Conceptos relacionados al sector salud

2.1.1.1.1 Acto médico

Se considera así a cualquier atención o acción que realice el personal médico como parte del ejercicio continuo de su profesión. Esto comprende el diagnóstico, terapia y pronóstico que realice el médico durante la atención de sus pacientes. (MINSA, 2005)

2.1.1.1.2 Atención de salud

Acciones que se brinda a los pacientes como procedimiento para promover, prevenir, recuperar o rehabilitar la salud de una persona. (MINSA, 2005)

2.1.1.1.3 Consentimiento informado

Documento físico en el cual el paciente – o su representante legal en caso de encontrarse imposibilitado – expresa su conformidad de manera libre y voluntaria sobre la atención de salud recibida. Para este fin el paciente debe haber sido informado sobre el tipo de atención además de los riesgos, efectos colaterales y beneficios que puedan generarse como consecuencia de la atención recibida. Este documento debe ser firmado y archivado para garantizar su validez legal. (MINSA, 2005)

2.1.1.1.4 Historia Clínica

Documento médico legal en el que se lleva un registro de los datos de identificación y de todos los procesos relacionados con las atenciones de salud que haya recibido el paciente. Es llenada por los profesionales de la salud registrando de manera secuencial los detalles de la atención brindada. Según la normativa vigente, la historia clínica debe tener la siguiente estructura: (MINSA, 2005)

1. Identificación del paciente

   También conocida como Hoja de Filiación, contiene los datos personales que identifican al paciente, incluyendo los datos de la organización prestadora de salud en la que se realiza la atención y el número de Historia Clínica generado.

2. Registro de la atención de salud

   Contiene los registros de las atenciones de salud que ha recibido el paciente a lo largo de su historial de tratamientos en la entidad prestadora de salud.

3. Información complementaria

   Se registran en esta sección los resultados de exámenes, análisis, documentos y consentimientos del paciente que se encuentren relacionados con su tratamiento o consultas en la entidad prestadora de salud.

2.1.1.1.5 Métodos de archivo de Historia Clínica

Se denomina así a las diferentes técnicas que se utilizan para organizar el Archivo Clínico de la organización prestadora de salud. Tiene por motivo mantener un orden que facilite el archivado y reconocimiento de las Historias Clínicas de los pacientes. (MINSA, 2005)

2.1.1.1.6 Información personal de salud

Este concepto se refiere a toda aquella información perteneciente a una persona usuaria de los servicios de salud y que describe sus características físicas o mentales, además de todo registro acerca de sus tratamientos, operaciones, medicaciones o servicios que ha recibido por parte de la institución médica correspondiente. Para fines del uso de la norma ISO 27799, se considera que la información personal de salud – en forma de lista no exclusiva – puede incluir los siguientes datos:

1. Información del registro del paciente.
2. Información sobre los pagos o elegibilidad del paciente para utilizar los servicios de salud de la institución.
3. El registro de identificación único del paciente en los sistemas de la institución.
4. Cualquier información sobre el paciente que haya sido recolectada a lo largo del uso de los servicios de salud.
5. Información derivada de los análisis o exámenes que se realicen al paciente o a sustancias o tejidos pertenecientes al mismo.
6. Identificación de una persona como profesional de la salud al paciente.

El concepto de Información personal de salud se aplica sin tener en cuenta el medio – ya sea digital, físico o audible – en el que los datos se encuentren almacenados. Es por este motivo que el Sistema de Seguridad a implementar no tendrá un alcance exclusivo de información digital puesto que en las entidades prestadoras de salud aún son muchos los datos que se almacenan físicamente. (ISO 27799, 2008)

2.1.1.1.7 Informática de salud

Es la disciplina científica que aplica la informática y tecnologías de comunicación para procesar la información médica necesaria que sirva de soporte a las operaciones de las instituciones del sector salud. En la actualidad constituye una de las más importantes herramientas utilizadas por las entidades prestadoras de salud dada la versatilidad y disponibilidad de la información que se logra mediante el uso de software especializado, permitiendo que la información de los pacientes se mantenga actualizada. (ISO 27799, 2008)

2.1.1.1.8 Sistema de Información de salud

Se considera así a cualquier sistema, repositorio o conjunto de datos – ya sean bases de datos, datawarehouse, etc. – que almacena información relevante sobre el cuidado de la salud de uno o más pacientes, y que se encuentra almacenada de tal forma que pueda ser transmitida de forma segura por parte de usuarios autorizados según su nivel de acceso a la misma. (ISO 27799, 2008)

2.1.1.2 Conceptos relacionados a la propuesta de solución

2.1.1.2.1 Activo de información

La definición primordial de activo es cualquier cosa que tenga valor para la organización, ya sean activos tangibles – equipos, muebles de oficina, vehículos, edificios, terrenos, etc. – como intangibles – software, datos, patentes, etc.

Como parte del análisis que se requiere para el diseño de un Sistema de Seguridad de la Información, se debe realizar un estudio de todos los activos críticos para el funcionamiento de la organización, centrándose en aquellos que generen, contengan o procesen información. Contextualizando el presente concepto al sector salud, se consideran activos los siguientes: (CNB - INDECOPI, 2008) (ISO 27799, 2008)

1. Información de salud.
2. Servicios y equipos de tecnologías de información.
3. Hardware y software de la organización.
4. Servicios y equipos de comunicación.
5. Dispositivos médicos que graban o generan reportes.

2.1.1.2.2 Riesgo

Definido en su forma más simple como una *situación* que expone a un *objeto* a que pueda ser *afectado o dañado*. Extendiendo más el concepto de riesgo, se puede determinar que ésta situación tiene cierto grado de *probabilidad* de generar un incidente en el cual el objeto de estudio – en el caso de un proyecto de SGSI sería el activo de información – pueda resultar afectado. De esta forma, en un sentido más amplio, se puede definir al riesgo como la combinación de la probabilidad de que ocurra un incidente con las consecuencias que generaría el mismo en el caso de que se materialice. (CNB - INDECOPI, 2008) (ISO 27799, 2008) (TALABIS & Martin, 2012) (ISACA, 2012) (PELTIER, 2005) (ISO 31000, 2013)

La situación en la cual existen probabilidades que son distintas para los riesgos identificados en un proyecto de este tipo, crea un estado de incertidumbre que genera la necesidad de realizar un análisis de riesgos. Como parte de la definición inicial se puede reconocer los siguientes

componentes del riesgo, los cuales están relacionados con los términos utilizados en dicha definición:

- Evento o incidente (*situación*)
  Referido a un evento futuro, del cual no se tiene certeza de que ocurrirá o no y que tiene una gran influencia en las consecuencias que puedan determinarse para el riesgo. La identificación de los eventos posibles es crítica en el estudio relacionado con el control de riesgos.

- Activo (*objeto*)
  Definido como algo que tiene un valor para la organización, es el objetivo directo o indirecto de un evento y como tal, se verá afectado por las consecuencias que se generen como materialización de este evento.

- Consecuencia (*daño*)

  Se define así al impacto que tiene sobre el activo, la ocurrencia de uno de los eventos que constituyan un riesgo para el mismo. Como tal supone un daño o potencial pérdida ya sea parcial o total del activo relacionado.

- Probabilidad

  Es la medición o valuación que se realiza sobre el riesgo, y que tiene como resultado un valor que permita determinar una métrica que sirva para catalogar y priorizar los riesgos, y así definir para cuáles es crítico establecer controles o cuales pueden ser aceptados.

La existencia del riesgo en conjunto con la incertidumbre que se generan como consecuencia del uso de probabilidades sumada a la gran cantidad de información que maneja una organización, requiere que se proceda a proteger los activos de información críticos – puesto que la protección de todos los activos supondría un gran trabajo y costo operativo. Para este fin se realiza un Análisis de Riesgos, el cual comprende las siguientes etapas:

1. Identificación y valoración de activos

   Comprende el estudio de los procesos de negocio que comprende las actividades de la organización objetivo para poder definir el alcance – el cual debería ser uno o más procesos críticos de negocio – que tendrá el presente análisis, a continuación se determinan los activos que cubre el alcance establecido. Para realizar el levantamiento de información que lleve a la definición del alcance y activos críticos se pueden utilizar herramientas como entrevistas, encuestas, documentación existente, etc. Como resultado de esta etapa se debería tener la documentación que especifique los procesos y activos sobre los que se centrará el Análisis de Riesgos.

2. Identificación y valoración de riesgos

   En base al alcance que se definió en la etapa anterior, se realiza un análisis de los riesgos y amenazas existentes. Dado que los riesgos pueden categorizarse en diferentes grupos dependiendo de su origen (naturales, humanos o del entorno), es importante que se utilicen

herramientas que puedan cubrir la mayor cantidad de posibilidades. Para este fin, se pueden utilizar checklist, revisión de la información histórica de los eventos e incidentes ocurridos y lluvia de ideas. Una vez determinadas las amenazas existentes, se procede a establecer la probabilidad de ocurrencia de cada uno, así como el impacto que generaría su materialización sobre los activos de información. Este último paso nos permitirá establecer una priorización de los riesgos según su criticidad o impacto en el negocio, sin embargo como resultado de este análisis puede escogerse aceptar algunos de ellos y no establecer controles para los mismos, ya sea por su bajo impacto o su poca probabilidad de ocurrencia.

3. Establecimiento de controles a implementar

   Utilizando la valorización y categorización de los riesgos encontrados en base a los criterios utilizados en el paso anterior, el paso final del análisis de riesgos es el establecer controles que minimicen el impacto del riesgo, o disminuyan la probabilidad de ocurrencia del mismo. Mientras más controles se identifiquen para un riesgo la mitigación del mismo será mayor, sin embargo es importante evaluar si los controles que se tienen pensados serán efectivos o no. Para este fin se debe realizar nuevamente un análisis del riesgo pero teniendo en cuenta los controles que se desee implementar como parte del contexto del mismo. De esta forma se podrá tener una medición de cuánto limita el riesgo cada control implementado.

2.1.1.2.3 MAGERIT versión 3

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información nace como una iniciativa por parte del Consejo Superior de Informática, entidad perteneciente al gobierno Español como respuesta a la regulación establecida en el Real Decreto 3/2010 – el cual regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Esta metodología de gestión de riesgos tiene los siguientes objetivos: (MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, 2012)

1. Concientizar a los responsables de las organizaciones sobre la presencia de riesgos y la necesidad e importancia de gestionarlos.
2. Ofrecer un método para analizar los riesgos a los que estén expuestos los activos de información.
3. Descubrir y planificar los controles a implementar para mitigar y controlar los riesgos.
4. Preparar a la organización para los futuros procesos de evaluación, auditoría o certificación que pueda requerir.

El esquema de trabajo que sigue la presente metodología permite cubrir todos los resultados referentes al análisis, documentación y control de los riesgos a los que se encuentra expuesta la información de la organización. Esto se puede ver en los pasos que la metodología establece para realizar el análisis de riesgos:

1. Determinar los activos relevantes para la organización, su interrelación y su valor (entendido como el costo de que éstos se vean afectados como consecuencia de algún riesgo).
2. Determinar las amenazas a las que se encuentran expuestos los activos identificados.
3. Determinar las medidas de protección actuales y la eficacia de las mismas frente al riesgo.
4. Estimar el impacto, es decir el daño que ocasionaría al activo de información la materialización de una amenaza.
5. Estimar el nivel de riesgo, el cual se calcula utilizando el impacto ponderado con la tasa de ocurrencia que se espera de la amenaza.

2.1.1.2.4 Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

Es una colección de herramientas, técnicas y métodos utilizados para el aseguramiento de riesgos de activos de información. Desarrollada por el *Software Engineering Institute*, las herramientas que pone a disposición para el análisis de riesgos presentan una complejidad muy alta, por lo que suele ser aplicada en entornos de gran escala. (TALABIS & Martin, 2012)

La metodología OCTAVE presenta 3 versiones diferentes:

1. OCTAVE

   Su uso se recomienda en el caso de realizar un análisis de riesgos a una organización de más de 300 empleados, además de requerir una gran capacidad para realizar evaluaciones de seguridad a nivel de toda la organización.

2. OCTAVE-S

   Es una versión desarrollada para organizaciones con menos de 100 empleados, su implementación requiere de un equipo de entre 3 a 5 personas que deben tener conocimientos sobre a los procesos operativos de la compañía, sus activos de información, requisitos de seguridad, riesgos y amenazas.

3. OCTAVE-Allegro

   Desarrollado de manera similar que la versión anterior, para empresas pequeñas, sin embargo ésta no requiere una participación organizacional muy amplia. Para su aplicación plantea los siguientes pasos:

   - Establecer criterios de valoración del riesgo

     Dado que el tipo de información crítica varía entre las diferentes empresas, cada una debe establecer una medida de valuación de los riesgos e identificar las áreas que puedan verse impactadas por las amenazas que puedan existir.

   - Establecer un perfil de activo de información

     Se realiza un estudio con la finalidad de identificar una lista de activos de información catalogados según la criticidad que representan para la organización, junto con la información respecto a sus dueños y sus requerimientos de confidencialidad, integridad y disponibilidad.

   - Identificar los contenedores de los activos de información

     Se deben identificar todos aquellos activos de la compañía que contengan información por sí mismos, como por ejemplo:

hardware, data centers, dueños de activos de información, técnicos, etc.

- Identificar las áreas de interés

  OCTAVE utiliza el término “áreas de interés” para identificar a todas aquellas situaciones que puedan afectar los activos de información de la organización. Dicho de otra forma se puede considerar como las debilidades o vulnerabilidades que existen en el sistema actual.

- Identificar los escenarios de amenazas

  Como consecuencia del paso anterior, se realiza un análisis de los escenarios que podrían darse como consecuencia directa de las vulnerabilidades identificadas.

- Identificar los riesgos

  Este paso busca establecer de una manera cuantitativa el nivel de riesgo que suponen las amenazas que se encontraron como parte del análisis anterior. El cálculo de esta valoración se realiza utilizando la amenaza en conjunto con el impacto al cual se relaciona.

- Analizar los riesgos

  En esta fase se otorga una puntuación a cada uno de los riesgos establecidos en el paso anterior. De esta forma se puede determinar la prioridad que tendrá cada uno de ellos en la implementación del plan de mitigación.

- Seleccionar un enfoque de mitigación

  En base a los valores asignados a los riesgos sobre los que se ha realizado el análisis, se procederá a elegir el modo de acción a seguir frente a cada uno de ellos. De esta forma se puede elegir mitigar el riesgo, postergarlo o aceptarlo.

2.1.1.2.5 ISO 31000

Estándar internacional que establece una guía general – sin establecer medidas específicas para algún tipo de actividad organizacional – para el tratamiento de riesgos, por este motivo puede ser utilizada de manera genérica en cualquier tipo de organización.

En su calidad de ser una guía generalizada de gestión de riesgo, puede ser aplicable a una gran cantidad de escenarios en diferentes organizaciones. Al igual que la norma ISO 27005, éste estándar sigue el ciclo de Deming (Plan-Do-Check-Act) como metodología de análisis de riesgos. (PASSENHEIM, 2010) (GIBSON, 2010)

2.1.1.2.6 Seguridad de la Información

Se denomina así al conjunto de políticas, estándares y controles que se implementan en la organización con la finalidad de asegurar la preservación de las siguientes propiedades de la información:

1. Confidencialidad

   Protección de la información confidencial del acceso o divulgación por parte de entidades – personas jurídicas o naturales – no autorizadas al mismo, tanto por parte del originario de la información como por parte de la entidad que maneja la misma.

2. Integridad

   Protección de la información frente a la modificación o eliminación sin la autorización o accesos necesarios. De esta forma se garantiza que la información sea la correcta en todo momento.

3. Disponibilidad

   La información se encuentra accesible en todo momento, bajo demanda de todo usuario que se encuentre autorizado a poder acceder a la misma.

4. Autenticación

   Mediante esta propiedad, se permite identificar a la persona o personas que han generado la información que se está verificando,

permite una validación en la autoría de la información por parte de un usuario específico.

5. No repudio
   Permite que la información sea validada a través de algún mecanismo que compruebe su integridad y contenido, declarándola como genuina.

Estas propiedades son las mínimas que un SGSI debe proteger para asegurar la información de la organización. (CNB - INDECOPI, 2008) (ISACA, 2012)

2.1.1.2.7 Sistema de Gestión de Seguridad de la Información

Este concepto, también nombrado SGSI, o ISMS – Information Security Management System – nace como respuesta a la necesidad de las empresas de proteger la información que es crítica para sus operaciones, tanto del acceso por personas no autorizadas como de daños producidos por las consecuencias de la materialización de los riesgos a los cuales esta se encuentra expuesta. Se encuentra muy relacionado con el plan de continuidad de negocios que se encarga de definir las acciones a seguir en caso un evento produzca una interrupción en las operaciones normales de la compañía.

A grandes rasgos el SGSI contiene la identificación de los activos de información que deban ser protegidos, el motivo por el que se deban proteger – es decir, la criticidad que éstos representan para la organización – los riesgos y amenazas ante los que se encuentran expuestos y los controles que se apliquen para asegurar la preservación de dichos activos. Al ser de vital importancia para las operaciones de la organización, se define también como *"la parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información"* (ALEXANDER, 2007).

Al requerir una identificación de los objetivos que se deban proteger, así como de todas las amenazas a las cuales se encuentran expuestos, y los

controles que deban implementarse, la implementación de un SGSI se realiza utilizando los resultados que se obtengan del Análisis de Riesgos. (ALEXANDER, 2007) (ORMELLA, 2013)

2.1.2 Marco regulatorio / legal

Como se explicó en la problemática del presente documento, el entorno sobre el cual se desarrollan las entidades públicas ha cambiado debido a la aprobación de nuevas normas que requieren su implementación siguiendo un calendario establecido. El marco legal que incumbe al presente proyecto de fin de carrera se encuentra compuesto por tres documentos aprobados y que se encuentran en vigencia actualmente. En esta sección se expondrá la explicación de las necesidades y los objetivos de cada uno de estos documentos.

2.1.2.1 Ley General de Salud, Código de ética y Deontología

La ley general de salud fue promulgada el 9 de julio de 1997 y publicada el 20 del mismo mes y nace como una iniciativa para reglamentar los servicios de salud ofrecidos por las instituciones correspondientes. Dicha norma se conforma de 6 títulos los cuales tratan los siguientes aspectos:

1. Derechos, deberes y responsabilidades concernientes a la salud individual.
2. Deberes, restricciones y responsabilidades en consideración a la salud de terceros.
3. Del fin de la vida.
4. De la información en salud y su difusión.
5. De la autoridad de salud.
6. De las medidas de seguridad, infracciones y sanciones.

Dentro del primer título, la presente ley establece en el "*Artículo 25.- Toda información relativa al acto médico que se realiza, tiene carácter reservado"* que el profesional de la salud, técnico o auxiliar que haga pública información relacionada a algún tratamiento médico es sujeto de sanción debido al rompimiento de los códigos de ética profesional

aplicados al desempeño de actividades médicas. Se establecen excepciones para esta norma en los siguientes casos.

- Consentimiento por parte del paciente.
- Solicitud de autoridad judicial.
- Uso con fines académicos, en este caso la información personal del paciente debe ser mantenida anónima.
- Información facilitada a familiares con fines de facilitar el tratamiento, previo consentimiento del paciente.
- En caso sea información que deba ser notificada de manera obligatoria, por ejemplo la infección por una epidemia.
- Cuando sea facilitada a la entidad aseguradora a la que se encuentra afiliado el paciente con fines de reembolso, beneficios, etc.
- En caso sea necesario para mantener la continuidad de la atención médica del paciente.

Como complemento a las disposiciones establecidas en ésta ley, el código de ética del Colegio Médico, establece disposiciones similares para el tratamiento de resultados médicos (Art. 23), la discusión respecto a casos médicos (Art. 63 inc. h) y datos que el paciente ha facilitado como parte de su tratamiento (Art. 89).

En concordancia con lo expuesto tanto en la ley como en el código de ética, se tiene el Artículo 165 del Código Penal Peruano el cual establece la pena correspondiente para el caso en que una persona revele información sin consentimiento del afectado, sería sujeto a una pena privativa de libertad de no más de dos años con sesenta a ciento veinte días. (CONGRESO DE LA REPÚBLICA, 1997) (PODER EJECUTIVO, 1991) (COLEGIO MÉDICO DEL PERÚ, 2007)

2.1.2.2 Lineamientos de políticas de Seguridad de la Información del Ministerio de Salud

Aprobado por el Ministerio de Salud mediante la Resolución Ministerial N° 520-2006/MINSA, nace como una iniciativa que sigue los lineamientos de la “Norma Técnica Peruana (NTP) ISO/IEC 17799:2004 Código de buenas prácticas para la gestión de la seguridad de la información” – la cual es un

precedente de la actual Norma Técnica Peruana ISO/IEC 27001:2008 – para integrar un método de protección de la información que el Ministerio de Salud y todas sus dependencias procesan y generan.

Esta norma se centra en la identificación de la información que se manipula como parte de los procesos críticos del Ministerio de Salud e instituciones afines a éste, exponiendo varios aspectos que se deben tener en cuenta para fortalecer la seguridad de la información, sirviendo a la vez de guía de aplicación de la NTP vigente en el año 2004.

Como parte de su desarrollo presenta el concepto de información – sin tener en cuenta exclusión alguna debido al tipo de medio en el que se almacene, es decir sea físico o digital – como un activo institucional que, correspondiendo al concepto de activo, supone un valor para la institución y debe ser clasificado para un mejor manejo del mismo.

Siguiendo el concepto de valor, se aplica la consideración de que todo elemento de éste tipo está sujeto a riesgos que deben ser controlados mediante mecanismos adecuados que permitan mitigar o controlar los efectos de dichos riesgos en caso se materialicen.

El documento además incorpora en el proceso de la gestión de seguridad a todos los integrantes de la organización, incluyendo tanto al comité de Alta Dirección como a los responsables y actores de los procesos de información.

Se considera importante la presente norma dentro del presente trabajo de investigación dado que es un precedente de las actuales normas que regulan actualmente la gestión de la seguridad en el sector salud.
Su alineación con las buenas prácticas expuestas en la NTP 17799:2004 y su aplicación en las dependencias del Ministerio de Salud permiten que las instituciones a las cuales afecta hayan realizado un trabajo inicial en lo que respecta al manejo de la seguridad de información. (MINSA, 2006)

2.1.2.3 Familia de Normas ISO/IEC 27000

La Organización Internacional para la Estandarización – ISO por sus siglas en inglés – se encarga de publicar estándares sobre diferentes temas que tienen una gran importancia en diferentes aspectos relacionados con el comercio, fabricación, etc. Siguiendo el constante crecimiento que ha tenido el desarrollo del campo de las Tecnologías de Información, dicho ente ha emitido varios estándares que regulan el ciclo de vida del software, estándares de calidad, sistemas de información y seguridad de la información.

Correspondiente a éste último grupo, se realizó la publicación de la familia de normas de la serie 27000, enfocadas directamente a la estandarización de los aspectos relacionados con la gestión de la seguridad de la información en las empresas y organizaciones que requieran contar con sistemas de gestión para este fin. A continuación se detallan las principales normas pertenecientes a esta serie, algunas de las cuales servirán de soporte para realizar los procesos requeridos para completar el presente proyecto.

- ISO 27001:2013, Information security management systems - Requirements
  Especifica los requisitos a cumplir para poder establecer el Sistema de Gestión de Seguridad de la Información.

- ISO 27002:2013, Code of practice for information security controls
  Presenta una guía de recomendaciones y buenas prácticas a seguir en la gestión de seguridad de la información.

- ISO 27003:2010, Information security management system implementation guidance
  Establece una guía de implementación para las normas de la serie.

- ISO 27005:2009, Information security risk management
  Centrada en presentar una metodología para el análisis de riesgos.

- ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002

Es una guía que extiende los conceptos y aspectos presentados en ISO 27002 aplicándolos al contexto específico de las entidades de salud.

Dado el alcance del presente proyecto, se utilizarán las normas ISO 27001 – como soporte de la implementación de lo indicado por la Norma Técnica Peruana 27001, la cual se detalla en la siguiente sección – ISO 27005 – como herramienta para cubrir el análisis de riesgos necesario para establecer el SGSI – e ISO 27799 – dada su especificación de conceptos en el contexto sobre el cual se desarrollará el proyecto. (ORMELLA, 2013) (ISO 27001, 2013) (ISO 27002, 2013) (ISO 27799, 2008)

2.1.2.4 Norma Técnica Peruana NTP ISO/IEC 27001

Es una norma elaborada por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos, publicada en el año 2009 y establecida como de uso obligatorio mediante la Resolución Ministerial N° 129-2012-PCM el año 2012, se encuentra alineada al estándar ISO/IEC 27001 - estándar internacional publicado en el año 2005 que provee un modelo a seguir para el establecimiento y mantenimiento de un SGSI. El objetivo principal de esta norma es establecer los requisitos que se deben cumplir para la implementación del SGSI utilizando un enfoque a procesos, lo cual requiere que se tenga disponible la mayor cantidad de documentación respecto a los mismos.

La norma utiliza la metodología Plan-Do-Check-Act – también llamado ciclo de Deming – para definir las fases de vida y mejora continua del SGSI a través de un seguimiento del mismo que asegura el mantenimiento de los controles y los cambios necesarios para poder mitigar los posibles nuevos riesgos que aparezcan luego de la implementación del sistema. A continuación se presenta un diagrama que detalla las etapas de esta metodología.

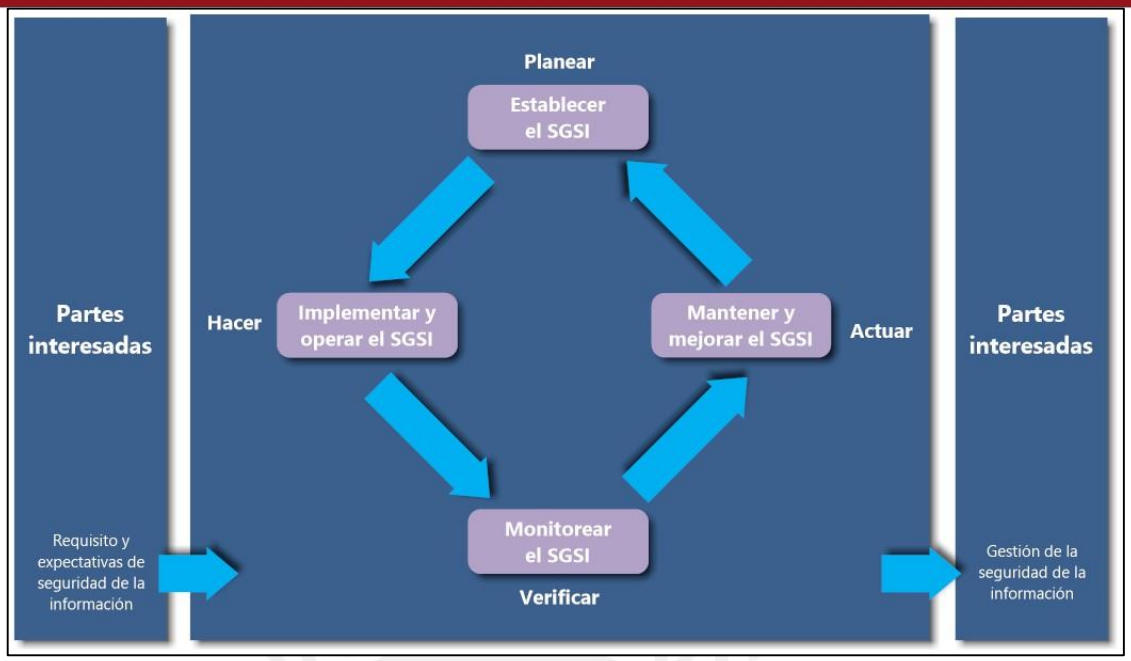

Ilustración 2 Estrategia de mejora continua del SGSI, Ciclo de Deming Fuente: Elaboración propia, basado en NTP ISO/IEC 27001:2008 (CNB - INDECOPI, 2008)

El diseño del SGSI siguiendo las fases del ciclo de Deming comprende las siguientes etapas:

- Establecimiento

  Se dan las recomendaciones a seguir para establecer el alcance que tendrá el sistema sobre la organización sobre la que se está trabajando. A continuación se realiza un análisis de identificación de activos de información en conjunto con los riesgos y amenazas a los que se encuentran expuestos, además de realizar la valoración tanto de los activos como de los riesgos asociados y los posibles controles que podrían implementarse para mitigar los mismos.

- Implementación

  En esta fase se implementan las políticas y planes de mitigación que se requieren para poder tratar el riesgo identificado en el alcance del sistema. Como parte de esta etapa se detallan las acciones específicas que se deben realizar como parte del plan de mitigación.

- Monitoreo y revisión

  El establecimiento de políticas que rijan los procesos desde el punto de vista de la seguridad de los activos de información que los mismos utilizan, requiere que se establezcan también métricas y procedimientos con los cuales se pueda evaluar su eficiencia y determinar si es necesario realizar algún cambio para mejorar su desempeño, el cual es el objetivo principal de esta etapa.

- Mantenimiento y mejora continua

  Luego de realizar las evaluaciones de desempeño del SGSI en la etapa anterior, se puede identificar cambios que son necesarios para reajustar el alcance o mejorar su eficacia en el control de riesgos. Esto, sumado a que el SGSI es una entidad que continua vigente a lo largo del tiempo de vida de la organización, hace que el mantenimiento del mismo sea una tarea crítica como parte de su ciclo de vida.

Recientemente, mediante la Resolución Ministerial N° 129-2012/PCM (PRESIDENCIA DEL CONSEJO DE MINISTROS, 2012), fue aprobado el uso obligatorio de esta norma para todas las entidades que pertenezcan al Sistema Nacional de Informática – entre ellas el Ministerio de Salud y todas sus dependencias – siguiendo el cronograma de implementación incremental determinado por la Oficina Nacional de Gobierno Electrónico e Informática, el cual determina las fases y duración del desarrollo de las mismas.

Para el presente proyecto de fin de carrera, además de seguir los requisitos establecidos por la presente norma. Debido a su carácter de obligatoriedad, está estrechamente relacionada con la problemática que ataca este proyecto y representa uno de los documentos más importantes a seguir durante el desarrollo del Sistema de Gestión de Seguridad de la Información. 2008 (CNB - INDECOPI, 2008) (ISO 27001, 2013) (ALEXANDER, 2007)

2.1.2.5 Ley de Protección de datos Personales

La Ley N° 29733 de Protección de datos personales publicada en julio del 2011 y siendo aprobada su aplicación en marzo del 2013, nace como respuesta a la necesidad de tener un documento que regule la manera en la que se hace uso de la información personal en los procesos de negocio de todas las organizaciones que realicen operaciones en Perú. Anteriormente se crearon diferentes normas que hablaban acerca de las limitaciones que se debería tener en cuenta para el manejo de la información personal de los clientes o interesados. Sin embargo, la falta de especificación en los casos, así como el carácter un tanto abierto de las sanciones que dichos documentos especificaban requirieron que se cree una norma más específica que sirva como ente reglamentario sobre la información personal.

Según detalla la ley, se considera dato personal a cualquier dato que pueda ser utilizado para identificar a una persona natural, de esta forma se puede considerar como datos personales el nombre de una persona, su dirección, su sexo, etc. Profundizando más en este concepto, se define además como dato sensible a aquellos que comprendan los datos biométricos, origen racial, religión, etc.

Si bien es cierto que dichos datos casi siempre son necesarios para poder acceder a algún servicio – ya sea financiero, educativo o de salud – la ley detalla que el titular de dichos datos tiene los siguientes derechos respecto de esta información:

- Solicitar información sobre el uso que se dará a la información que facilite.
- Solicitar acceso a la información que la organización posee sobre él.
- Solicitar la actualización, rectificación, adición o supresión de datos.
- Solicitar que su información personal no sea suministrada a terceros.

A pesar de constituir una medida de protección para la información de las personas naturales, cabe destacar que ejercer muchos de estos derechos conlleva a un pago para poder hacerlos cumplirse.

Como objetivo respecto al reglamento que establece esta ley, se menciona a los dueños y encargados de los bancos de datos personales – también denominados sujetos pasivos, tanto de la administración pública como privada – los cuales deberán modificar sus procedimientos para poder cumplir los requerimientos de esta norma.

Se señala además que aquellos bancos de datos que sean de uso privado, así como los que se utilicen para las operaciones de la administración pública – incluidas las que soportan los procedimientos de defensa nacional, seguridad pública e investigación penal – se encuentras exceptuadas de la aplicación de la norma.

El principal objetivo de la norma es que las personas naturales puedan tener conocimiento de quién tiene acceso a su información personal, además de conocer el tipo de uso que se le dará. De esta forma establece como garantía principal que el uso de datos personales debe estar sujeto al conocimiento – previo, informado, expreso e inequívoco – por parte del titular de dicha información. Sin embargo dicha garantía puede quedar invalidada en el caso que el ejercicio de éste derecho afecte, por ejemplo, intereses de terceros o investigaciones judiciales.

Dado su carácter de ley, todas las instituciones públicas o privadas que se encuentren en operación, deben garantizar el cumplimiento del reglamento especificado por la misma. (CONGRESO DE LA REPÚBLICA, 1997) (HUERTA, 2011)

2.2 Estado del Arte

El campo de acción respecto a los estándares de seguridad de la información enfocados al sector salud en el entorno nacional es relativamente reciente, como se ha podido observar en el marco legal presentado, las normas que regulan el uso y manejo de la información confidencial en el sector salud se hacen presentes a partir del año 2006, siendo reforzadas el año 2012 con la NTP 27001. Es por este motivo que el estudio del estado del arte es de difícil acceso en el entorno nacional y, sumado al enfoque del actual proyecto que utilizará una norma internacional, se ha realizado un estudio del estado del arte a nivel internacional.

Globalmente las iniciativas que han buscado proteger la información utilizada en los procesos que utilizan información personal han tomado distintos enfoques dependiendo de las propias normas y leyes de cada país. Es por este motivo que no existe un estándar mundialmente aceptado que pueda utilizarse para cubrir las diferentes necesidades de cada país, ocasionando que las diferentes metodologías utilizadas se hayan modificado para cumplir las normativas respectivas. En las siguientes secciones se procederá a describir las principales soluciones que se han implementado en diferentes países respecto a la protección de datos personales e información de salud.

2.2.1 Formas exactas de resolver el problema

Se consideran como formas exactas, a aquellas soluciones cuyo objetivo es resolver el problema directamente. En una revisión de la bibliografía existente se ha podido encontrar los siguientes casos de aplicación en entornos del sector salud.

2.2.1.1 Estudio de aplicación de la norma ISO/DIS 27799 en el SGSI de la industria del cuidado de salud

La norma ISO 27799 nace como una extensión de la norma ISO 27002 – la cual presenta una serie de buenas prácticas y recomendaciones a seguir para la gestión de la seguridad de la información – aplicando los conceptos de dicho estándar a la protección de la información utilizada en los procesos que llevan a cabo las organizaciones prestadoras de salud. En el caso mencionado en la referencia del presente ítem, se explica el proceso de implementación de la norma ISO 2779, acoplándolo a las normas CNS (Chinese National Standards) y HISPP/GD (Health Informatics Security and Privacy Protection guideline draft) vigentes en China.

En el desarrollo del estudio se especifica el concepto de HIS (Healthcare Informatics Security) como todos aquellos controles que se hayan definido en las operaciones de la entidad prestadora de salud para asegurar la seguridad de sus sistemas de información – de manera similar a un SGSI. El HIS de cualquier entidad de este tipo debe tener los siguientes objetivos:

1. Proteger la información personal.
2. Prevenir errores en la práctica de los servicios de salud.
3. Mantener las funciones de los órganos prestadores de salud (continuidad de los servicios de salud).

Para poder alcanzar estos objetivos, se realiza un análisis de vulnerabilidades, amenazas y riesgos del HIS, en el que se determinan los activos de información que deban ser protegidos contra éstos. Se presentan cuatro alternativas para el manejo del riesgo en este caso:

1. Establecer controles para los riesgos identificados.
2. Realizar una transferencia del riesgo hacia otra compañía. Como ejemplo a través de contratos que tercericen la gestión de riesgos.
3. Aceptar el riesgo latente sin necesidad de aplicar controles para evitar su materialización.
4. Tomar medidas que busquen evitar el riesgo en los casos en los que no se haya podido establecer medidas de control apropiadas.

Cabe resaltar que el estudio pone especial énfasis en análisis de riesgos que se debe hacer sobre el Centro de emergencias de la organización en la cual se pretende implementar la norma dado que es uno de los servicios de mayor importancia para un centro de salud y de vital importancia en la atención que necesiten los pacientes que han sufrido algún accidente y requieran atención inmediata.

Luego de realizar el análisis de riesgos de información, la metodología requiere que se elija un framework para la implementación de las políticas del SGSI. Estas políticas deben cubrir una serie de campos de acción, entre los principales: la política de seguridad de la información, la política del sistema de gestión de seguridad de la información, política de incidentes de seguridad de la información y la política de seguridad de sistemas de la información.
Como se puede observar, la metodología a utilizar en el caso de la aplicación de la norma ISO 27799 es bastante similar a la aplicación de la norma ISO 27001, la cual se detalla en el marco teórico. (FARN, Hwang, & Lin, 2007)

2.2.1.2 Protección de los datos personales de la historia clínica en Argentina y Uruguay e IHE XDS

En materia de protección de datos personales, y la legislación referente a la historia clínica de los pacientes de las entidades prestadoras de salud, tanto Argentina como Uruguay comparten muchas similitudes en cuanto a las normativas que rigen estos aspectos.

La problemática presentada en este estudio se localiza en el contexto de la publicación de una ley de datos personales en ambos países que obligaba

a las instituciones a acoplar su reglamento a los procesos cotidianos de las instituciones, entre ellas las del sector salud. Dicha ley, de manera similar a la ley de protección de datos publicada en Perú, tiene como centro el consentimiento del uso de la información por parte de la persona natural a la cual pertenece.

Esta nueva normativa conlleva la necesidad de adaptar los SGSI según lo que la norma obliga a cumplir. Para el estudio presentado se utilizó un modelo de integración denominado IHE (Integrating the Healthcare Enterprise), el cual es una iniciativa para integrar los distintos sistemas de información de diferentes organizaciones, mejorando la comunicación entre ellos.

Este modelo utiliza flujos reales de información en la institución, y busca formas de estandarizarlos para poder asegurar la transmisión de la información entre distintos sistemas.

La metodología presentada en este estudio comprende los siguientes puntos:

1. Definición de los cuatro grupos de datos necesarios para la implementación de la protección de datos personales.
   a. Consentimientos de los usuarios para el uso de su información personal.
   b. Datos de identificación de los pacientes.
   c. Datos comunes pero que requieren el consentimiento del usuario para su uso.
   d. Datos de las transacciones de la información de los pacientes que requieran el consentimiento de los mismos.

2. Establecer los actores que participan en el modelo IHE según cada grupo de datos de la etapa anterior.

3. Estudio de la flexibilidad de los sistemas que realizan el registro de los consentimientos de los usuarios.
4. Establecer los casos de acceso a la información personal.

a. Por parte del paciente, familiar, personal administrativo o médico tratante.
b. Por parte de un médico de otra institución.
c. Como información utilizada para un estudio científico.

Finalmente el estudio presenta las consideraciones a tener en cuenta en cada uno de los casos de acceso definidos como parte de la etapa final de la metodología.

El modelo presentado en el presente estudio permite tener un precedente del tipo de metodologías a utilizar en el caso del establecimiento de nuevas normas que afecten los sistemas de seguridad de la información previamente establecidos. (GIUDICE, Fauquex, Scotti, & Yelen, 2011)

2.2.2 Formas aproximadas de resolver el problema

Como formas aproximadas de resolver el problema, se presentan diferentes casos de normas o leyes que se han implantado en otros países y que no son aplicadas directamente a un tipo de organización, sino que son especificadas de manera general para que su uso pueda implantarse en diferentes organizaciones. En esta categoría se presentan los siguientes casos:

2.2.2.1 Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Traducida como Ley de Portabilidad y Responsabilidad del Seguro Médico, es un acta del sistema legislativo americano aprobada en el año 1996. En conjunto con el Departamento de Salud y Servicios Humanos de EE.UU. – US Department of Health and Human Services HHS – especifica un grupo de reglas que deben ser implementadas por todas aquellas instituciones que proveen servicios de salud con los siguientes objetivos:

1. Crear un sistema simple y más estandarizado que eventualmente disminuya los costos de los cuidados de salud.
2. Reducir los errores a través de una comunicación segura y universalmente aceptada de las transacciones de atención de salud.
3. Eliminar reclamos.

Las entidades que deben alinearse bajo esta normativa incluyen a todas aquellas que provean o estén relacionadas con los procesos de servicios de salud, entre ellas podemos nombrar:

- Planes de Salud, similares a los planes de seguros que se pueden encontrar en Perú, incluyen planes dentales, de visión entre otros.
- Proveedores de atención médica, tanto hospitales como consultorios privados.
- Centros de Información de Salud, instituciones que reciben información de clientes que se requieren para algún proceso relacionado con el cuidado de la salud, como por ejemplo servicios de cobranza.

Esta norma legal, se centra en el manejo de la información de los clientes utilizando las siguientes reglas:

1. Regla de privacidad
2. Regla de seguridad
3. Regla de transacciones y grupos de códigos
4. Regla de aplicación
5. Regla de identificador único

Entre este grupo de reglas, el desarrollo de los lineamientos directamente relacionados con Seguridad de la Información se dan en las primeras dos:

- Regla de privacidad
  Establece estándares sobre el uso y divulgación de la información de salud de los clientes – llamada Información de Salud Protegida – su objetivo principal es establecer cómo la información debe ser protegida apropiadamente a la vez que se permita el flujo de ésta para brindar un servicio de calidad.

- Regla de seguridad
  Enfocada a establecer estándares para el aseguramiento de toda información de salud que se encuentre en forma electrónica. Tiene como objetivo principal la protección de la información mientras se permite que las instituciones reglamentadas por esta norma puedan implementar nuevas tecnologías que permitan mejorar el nivel de servicio hacia los clientes.

En su calidad de norma legal, HIPAA ha tenido que ser aplicada a todas las instituciones que se encuentren dentro de la clasificación que se detalló en párrafos anteriores – tanto entidades públicas como privadas, incluyendo consultorios personales – requiriendo una fuerte inversión por parte de dichas organizaciones debido a cambios en los procesos, integración y cambios de sistemas que no cumplían con la normativa e implementación de controles. (SHONIREGUN, Dube, & Mtenzi, 2010) (UNITED STATES CONGRESS, 1996)

2.2.2.2 Japanese Personal Data Protection Act 2005 (JPDP)

El Acta de Protección de Datos Personales es una norma legal promulgada en Japón en el año 2005 como una respuesta a la necesidad de limitar la forma en que la información personal era manipulada y compartida sin tener en cuenta los principios de privacidad y seguridad.

Esta ley regula a todas aquellas entidades que manipulan información de un número mayor o igual a los cinco mil clientes, ya sea exclusivamente de nacionalidad japonesa o a nivel mundial. El enfoque que utiliza es un tanto distinto al de las demás normas que regulan la seguridad en temas de salud a nivel mundial, debido a que su forma de determinar la información crítica depende directamente de la institución que regula. Éste concepto puede entenderse mejor al explicar las principales normas que establece el acta para las empresas que regula (LEGISLATURA BI-CAMERAL JAPONESA, 2005):

1. Las empresas deben definir un “propósito de uso” que especifique cómo la entidad utiliza la información personal de sus clientes, constituyendo la base de los límites que dicha entidad tiene para el manejo de dicha información.

2. Se debe tener el consentimiento explícito de sus clientes para utilizar su información personal, dejando de lado el propósito de uso que tengan definido para la misma. De igual manera, se requiere la autorización del cliente en los casos en que se necesite proveer esta información a terceros.

3. Se debe implementar los controles de seguridad necesarios que prevengan la fuga, pérdida o daño de la información personal.

En conjunto con estas definiciones, el acta señala una lista de medidas respecto a la seguridad que deben ser cumplidos para garantizar la protección de la información sensible, las cuales se extienden a nivel de organización, personal de la empresa, seguridad física – gestión de la entrada y salida de personal para prevenir la fuga de información – y técnico.

El caso del Acta Japonesa de Protección de Datos Personales utiliza un enfoque muy distinto al presente en la mayoría de las normas que otros países han planteado respecto a este tema, principalmente por trabajar en base a los propósitos definidos directamente por las entidades que regulan. Es por este motivo que se presenta una dificultad al momento de plantear mecanismos de trabajo en conjunto entre instituciones regidas bajo este esquema con aquellas de otros países que se rigen bajo normativas distintas. (SHONIREGUN, Dube, & Mtenzi, 2010) (LEGISLATURA BI-CAMERAL JAPONESA, 2005)

2.2.2.3 UK Data Protection Act 1998 (DPA)

El Acta de Protección de Datos del Reino Unido es una norma establecida en el año 1998 como respuesta a la Directiva de Protección de Datos de la Comunidad Europea (1995). Regula directamente el aseguramiento del proceso de información personal de los usuarios afectados.

Esta normativa no especifica un rubro particular de entidades que deban regirse por los principios que presenta, en vez de ello determina que cualquier entidad que realice procesos de información personal debe implementar las medidas necesarias para alinear sus procesos a lo que recomienda el acta. Además indica que los dueños de la información que se utilice – es decir, aquellas personas cuya información está siendo utilizada por dichas instituciones – tienen derecho a pedir que se les informe qué datos personales se tienen y cuáles son las actividades que se están realizando con ellos.

La DPA especifica una serie de principios de protección de datos que se deben seguir como medidas normativas en los procesos de negocios. A continuación se detallan las consideraciones que las entidades afectadas deben tener en cuenta sobre la información personal que procesan (INFORMATION COMMISIONER'S OFFICE, 2011):

1. Debe ser procesada transparente y siguiendo las normas legales relacionadas.

2. Debe ser obtenida solo con uno o más propósitos específicos y legales, no debiendo ser procesada en cualquier manera que sea incompatible con estos propósitos.

3. Debe ser adecuada, relevante y no excesiva en relación al propósito o propósitos para los que será procesada.

4. Debe ser precisa y, cuando sea necesario, mantenerse actualizada.

5. La información procesada no debe ser mantenida por periodos de tiempo más largos de lo necesario para cumplir los propósitos por los cuales se obtuvo.

6. Debe ser procesada de acuerdo a los derechos de los interesados que se definen en el acta.

7. Se deben tomar las medidas técnicas y organizacionales necesarias contra el procesamiento desautorizado o que no rompa las normas legales, además de la pérdida, destrucción o daño de la información personal.

8. No debe ser transferida a un país fuera del Área Económica Europea, a menos que dicho país asegure un adecuado nivel de protección de los derechos y libertades de los interesados en relación al procesamiento de su información personal.

La norma DPA al ser de aplicación inmediata, ha generado que las instituciones del Servicio Nacional de Salud del Reino Unido – quienes se encuentran en un proceso de reestructuración desde principios del año 2013 – tengan que revisar sus procesos alineándolos a las recomendaciones y principios promulgados en esta nueva norma. (SHONIREGUN, Dube, & Mtenzi, 2010) (INFORMATION COMMISIONER'S OFFICE, 2011)

2.2.3 Conclusiones sobre el estado del arte

Como se puede verificar, las formas de afrontar la problemática respecto a la protección de la información en general han tenido enfoques distintos dependiendo de la legislación vigente en cada país. Es importante además señalar que no hay un consenso a nivel global sobre los mejores estándares a seguir para implementar un sistema de gestión de seguridad de la información debido a la variedad de normas y enfoques que se le da al concepto de seguridad.

Bajo este enfoque es importante que el sistema a implementarse cumpla con todas las normativas vigentes, evitando posibles problemas legales que puedan dañar la imagen de la compañía e incluso conllevar a multas debido al incumplimiento de las leyes locales. De esta manera se tiene que el uso de las normas internacionales siempre debe someterse al cumplimiento de la legislación correspondiente, teniendo que modificarse ciertos aspectos para ello.

Sería difícil aplicar las metodologías vistas en el estado del arte sin el trasfondo y soporte de las normas a las que responden; si bien es cierto que la principal norma que empuja a las instituciones públicas en Perú a implementar un SGSI está alineado a una norma internacional, su publicación en calidad de Resolución Ministerial hace que dicho estándar quede por debajo de leyes que deben cumplirse prioritariamente – entre ellas la Ley General de Salud y la Ley de Protección de Datos Personales – las cuales tienen un mayor peso por encima de este tipo de resoluciones.

Es así que el presente proyecto pretende realizar un análisis y diseño que permita la implementación de un SGSI a medida para una institución del sector salud, que a la vez cumpla con las leyes y normas superiores que rigen aspectos similares a los que el presente proyecto pretende dar solución.

3 CAPÍTULO 3: Documentación exigida por la norma ISO/IEC 27001:2013

En el presente capítulo se muestra los documentos requeridos por la norma ISO/IEC 27001:2013 que servirá como entrada al desarrollo del análisis y diseño del SGSI.

3.1 Caso de Negocio

El Caso de Negocio presentado a continuación tiene por finalidad hacer una revisión del estado actual del Instituto Nacional Materno Perinatal, identificando los agentes impulsores de cambio, las necesidades que tiene dicha institución en cuanto a Seguridad de la Información, la pertinencia del proyecto respecto a los objetivos del Plan Estratégico Institucional y la determinación del alcance preliminar para el desarrollo del proyecto.

Cabe destacar que el modelo utilizado para la creación del presente Caso de Negocio establece una serie de secciones recomendadas mas no mandatorias, siendo parte del proceso la elección de las secciones que sean pertinentes para el caso específico que se quiera presentar.

3.1.1 Necesidades del Negocio y descripción del proyecto

Problemática y Oportunidad del Proyecto

Las empresas que desarrollan sus actividades en el sector salud prestan un servicio crítico a la sociedad que es utilizado día a día por miles de personas que ponen incluso su vida en las manos del personal médico que los atiende. Estas atenciones a pesar de presentarse en distintas especialidades – cirugía, neumología, neurología por nombrar algunas – deben ser registradas por disposición legal en la Historia Clínica del paciente el cual debe ser almacenado en un registro físico que puede ser utilizado incluso en un proceso judicial.

El detalle de la información mínima requerida que debe ser almacenada en éste documento – incluyendo los formatos utilizados para registrar los diferentes tipos de atención – se encuentra descrito en la Norma Técnica de Historias Clínicas (MINSA, 2005), publicada por el Ministerio de Salud quien además da libertad a las instituciones bajo su jurisdicción a agregar datos adicionales y modificar el formato de dichos documentos.

Dicha norma adicionalmente contiene una serie de directivas que establecen las consideraciones que las instituciones deben tener en cuenta para el manejo de las Historias Clínicas de sus pacientes, entre las cuales podemos resaltar aquellas referentes a la custodia, entrega de copias e información, almacenamiento y depuración de las mismas que son de mucho interés en el desarrollo del presente proyecto.

En adición a las disposiciones previas el INMP se enfrenta a la necesidad de cumplir con la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 en cuya publicación se establece explícitamente que dicha institución, como parte del Sistema Nacional de Salud, debe proceder con el proceso de implementación de un Sistema de Gestión de Seguridad de la Información que garantice la Confidencialidad, Integridad y Disponibilidad de la información que se utilice como parte de sus procesos de negocio.

Además la promulgación de la Ley de Protección de Datos Personales modifica el escenario sobre el cual debe realizarse la implementación ya comentada, debiéndose además asegurar el cumplimiento de lo estipulado por dicha ley. Se debe tener en cuenta que el activo de información más

importante que maneja una entidad prestadora de servicios de salud es la Historia Clínica, la cual contiene tanto información personal como sensible de los pacientes que debe ser resguardada y utilizada bajo el consentimiento de los mismos.

Haciendo un análisis de la situación presentada, podemos observar que el principal agente impulsor del cambio es el Cumplimiento Normativo aplicado a las nuevas leyes promulgadas, lo cual conlleva a una mejora en la atención del cliente final dado que su información será resguardada, evitando filtraciones o pérdidas que puedan impactar negativamente su atención o intereses personales.

Según el cronograma de despliegue establecido junto con la Norma Técnica Peruana NTP ISO/IEC 27001:2008 para la implementación del SGSI en las entidades públicas, se puede observar la urgencia por iniciar las actividades requeridas para iniciar dicha labor, dado que la institución de salud objetivo se encuentra preocupantemente retrasada en el proceso, habiendo finalizado el plazo para la quinta y última fase, al término del desarrollo del presente documento, tal como se muestra en la siguiente línea de tiempo.

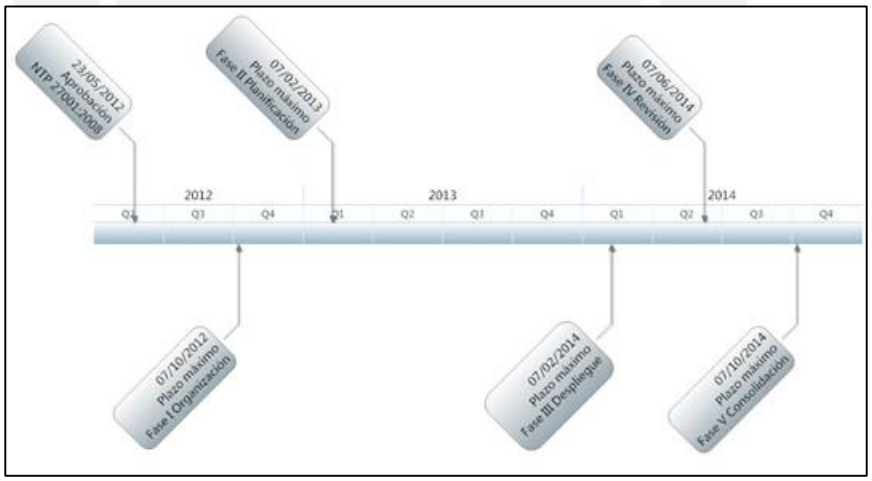

Ilustración 3 Cronograma establecido para la implementación del SGSI para las instituciones normadas por la NTP-ISO/IEC 27001:2008 Fuente: Elaboración propia, basado en el diagrama de Implementación incremental publicado en la Resolución Ministerial N° 129-2012-PCM (PRESIDENCIA DEL CONSEJO DE MINISTROS, 2012)

Es sobre este escenario que se presenta el presente proyecto, el cual pretende brindar a dicha institución una solución de implementación de un SGSI que cumpla adicionalmente con lo estipulado por las normas propias promulgadas por el Ministerio de Salud como por lo dictado en la Ley de Protección de Datos Personales.

Alcance preliminar

El proyecto presentado tiene como alcance realizar el Análisis y Diseño de un Sistema de Seguridad de la Información utilizando para ello la Norma ISO/IEC 27001:2013, teniendo en cuenta el cumplimiento de lo requerido por la Ley de Protección de Datos Personales.

En cuanto a los procesos de negocio que se analizarán para la definición de los entregables posteriores, el proyecto se enfocará en:

1. Proceso de Admisión de Pacientes.
2. Proceso de Emisión de Copia de Historia Clínica.

Limitaciones al Alcance

Dado que el proceso de implementación requiere un equipo de personas capacitadas, además de una inversión por parte de la institución, no se está considerando como parte del alcance.

Stakeholders[1]

Para el presente proyecto se ha identificado a los siguientes actores como principales interesados en cuanto a la ejecución del mismo:

- Instituto Nacional Materno Perinatal: en su calidad de entidad pública sujeta al cumplimiento de la legislación actual. El análisis y diseño realizado en el presente proyecto servirá como una base inicial que sirva de guía para el proceso formal de implementación del SGSI.

- Personal del área de Admisión: en su calidad de responsables legales del flujo de información relacionado con las Historias Clínicas. El

[1] Puede ser traducido como “interesados”. Se refiere a aquellos a quienes afectará de alguna manera la puesta en marcha del proyecto.

conocimiento y aplicación de los conocimientos detallados a lo largo del análisis realizado apoyara a mejorar la eficiencia de la labor realizada en el área, asegurando tanto el cumplimiento normativo como el aseguramiento de las Historias Clínicas.

- Pacientes de la entidad prestadora de salud: en su calidad de dueños de la información almacenada en las Historias Clínicas. La implementación futura de un SGSI garantizará que la entidad a la que acuden por servicios de salud mantengan la confidencialidad de la información incluida en sus Historias Clínicas, mejorando el nivel de servicio al cliente minimizando los casos de pérdidas que afecten a su servicio.

Alineamiento estratégico

El análisis y diseño de un SGSI será un proyecto alineado a los objetivos de negocio establecidos en el Plan Estratégico Institucional de la entidad prestadora de salud. Se ha identificado como el objetivo estratégico general sobre el cual se debería considerar la inclusión del presente proyecto el siguiente:

"Consolidar las actividades de gestión asistencial, administrativa, capacitación e investigación en el ámbito interno para optimizar la atención altamente especializada a los usuarios del Instituto" (INMP, 2012)

Este objetivo cuenta además con los siguientes objetivos específicos a los que se acopla como soporte el presente proyecto:

- Impulsar las actividades de mejora continua de la calidad en los procesos de atención a los pacientes.
- Fortalecer la gestión de la información.
- Afianzar los procesos de gestión administrativa.

Justificación del proyecto y recomendaciones

Según lo anteriormente expuesto, se puede realizar un análisis sobre la necesidad actual que tiene la institución prestadora de salud a la cual se pretende responder con el desarrollo del proyecto presentado.

De esta manera podemos observar que el manejo de la información de las Historias Clínicas es de vital importancia para realizar las principales actividades relacionadas al proceso de negocio principal que son aquellas relacionadas con la atención de pacientes. Es así que se identifica al área de Admisión como una de las más críticas desde el punto de vista de la seguridad de la información y el cumplimiento de las normas relacionadas a la confidencialidad y protección de información sensible de los usuarios.

Como ya se ha explicado, el activo de información principal de los procesos de negocio relacionados con el área de Admisión es la Historia Clínica de los pacientes, que mantiene los datos personales y sensibles de los mismos, entre los cuales podemos nombrar explícitamente a la Hoja de Filiación y a los diferentes formatos que detallan las atenciones recibidas en la institución.

Cualquier filtración de ésta información a agentes no autorizados – ya sea por la definición de los accesos del flujo de negocio o por consentimiento explícito del paciente – afectaría el pilar de seguridad de la información de la Confidencialidad, pudiendo derivar en acciones legales por parte de las partes afectadas que pueden conllevar además a la imposición de penalidades por incumplimiento de las normas legales vigentes.

Respecto a la Integridad, podemos afirmar que los cambios en la información detallada en las Historias Clínicas de forma arbitraria – es decir en el caso en que se modifique algún dato de la misma – pueden ocasionar inconvenientes en la atención de los pacientes incluso pudiendo poner en riesgo su vida en el caso que se haya modificado o retirado información respecto a alergias, análisis anteriores o diagnósticos.

De manera similar, un evento que afecte la Disponibilidad de ésta información afectará además de la calidad de atención al cliente, los tiempos de respuesta en casos de emergencia o el tiempo de espera para la atención en consultorios externos. Las consecuencias de ambos escenarios podrían también conllevar a penalizaciones y demandas por parte de los afectados.

Como ya se ha detallado en secciones anteriores el INMP se encuentra sujeto a la Resolución Ministerial N° 129-2012/PCM, en la que se establece explícitamente el nombre de la misma en el grupo de entidades públicas que deben seguir el cronograma establecido y publicado con dicho documento. De igual manera la institución debe cumplir lo estipulado en la Ley de Protección de Datos Personales dado que almacena información personal y sensible relacionada con el acto médico realizado en las atenciones a los pacientes, así como los diagnósticos y resultados de análisis de laboratorio, rayos x, ecografías entre otros.

Por los motivos expuestos se recomienda al INMP que se inicien las actividades para realizar el Análisis y Diseño del Sistema de Gestión de Seguridad de la Información requerido por la ley estableciendo para este fin un Comité de Seguridad de la Información que sea el encargado de realizar la Planificación, puesta en marcha y seguimiento del proyecto.

3.2 Alcance del SGSI

Alcance Organizacional

Por su naturaleza, las entidades prestadoras de servicios de salud realizan sus atenciones en ambientes en los cuales se dificulta el control sobre el público que accede entre los cuales se tiene pacientes, visitas, médicos, trabajadores y público en general, siendo difícil la segmentación de las personas que pertenecen a cada uno de estos grupos. El Instituto Nacional Materno Perinatal no es la excepción a éste paradigma, siendo uno de los servicios más caóticos en cuanto a cantidad de personas que acceden el Servicio de Admisión y Consultorios Externos.

Las funciones de las áreas involucradas en este servicio son los siguientes:

1. Servicio de Admisión

   Se encarga de gestionar la creación, mantenimiento, custodia, archivo, entrega y recepción de las Historias Clínicas de las pacientes que siguen tratamiento en cualquiera de los servicios del hospital – ya sea Consultorios Externos, Emergencia, Hospitalización, Cuidados Intensivos – además gestiona la generación de citas de las pacientes que realizan sus controles en Consultorios Externos.

2. Consultorios Externos

   Consultorios dedicados a la atención ambulatoria de las pacientes en diferentes especialidades como parte de sus controles pre y post natales. Entre ellos tenemos: medicina preventiva, vacunas, psicología y ginecología.

Como se ha explicado en anteriores secciones del presente documento, se ha identificado a la Historia Clínica como el activo de información más importante en los procesos del hospital. Este documento se ve expuesto a distintos riesgos, entre los cuales influye la ya mencionada cantidad de personal que se encuentra en el área cercana a Admisión, así como el poco control específico para el manejo de dicha información. Por este motivo se ha establecido realizar el análisis y diseño sobre los procesos más críticos de dicha área relacionados a la gestión de Historias Clínicas.

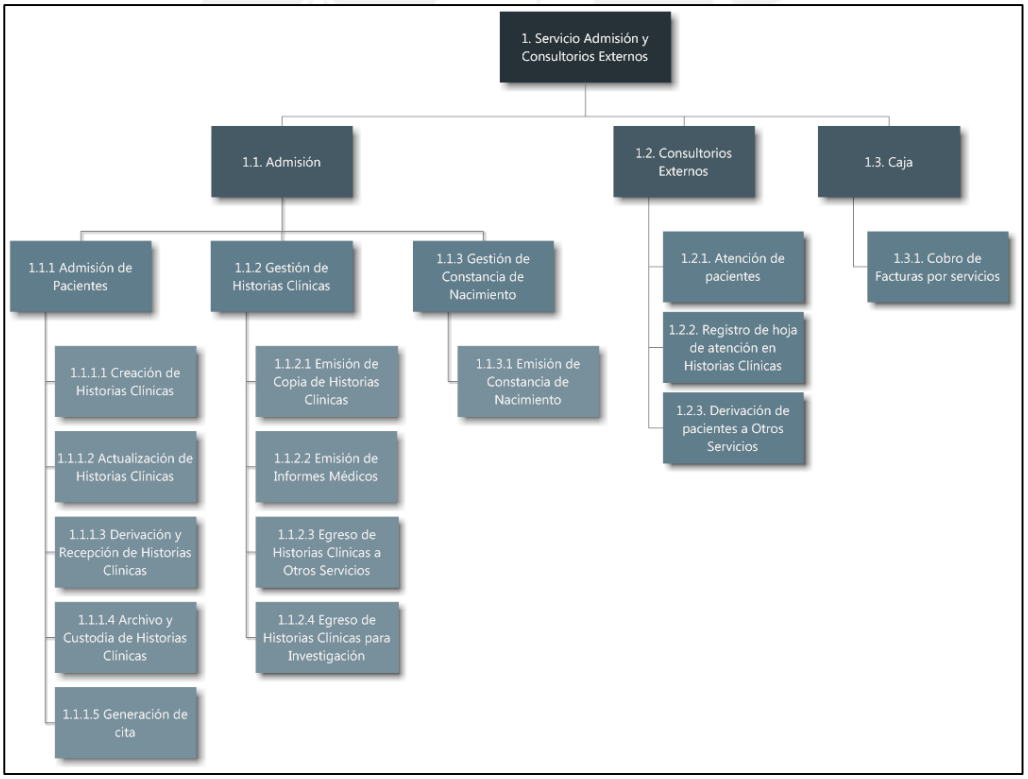

Ilustración 4 Funciones del Servicio de Admisión y Consultorios Externos Fuente: Elaboración propia

El servicio de Admisión y Consultorios externos se encuentra localizado en la entrada “Atención Ambulatoria” en el Jirón Miró Quesada en el Centro de Lima. Su función principal es prestar servicios de atención médica ambulatoria a pacientes que realizan sus controles pre y post natales recibiendo diariamente una gran cantidad de personas entre pacientes y familiares. La segregación de funciones y procesos de negocio en las áreas de este servicio son los siguientes:

Debido a las limitaciones de tiempo establecidas para el desarrollo del proyecto, se ha limitado el alcance a 2 procesos de negocio pertenecientes al área de Admisión. Los procesos escogidos son:

1. Admisión de Pacientes.
2. Emisión de Copia de Historias Clínicas.

Estos procesos escogidos han sido modelados utilizando la notación BPMN 2.0 de forma que se pueda tener la visión completa de las áreas y actores participantes de los mismos, así como el flujo de la información crítica escogida en el alcance. En el capítulo siguiente se mostrarán los procesos modelados, así como las conclusiones obtenidas del análisis realizado durante su elaboración, referido al aspecto de seguridad de la información.

Alcance en Tecnologías de Información y Comunicación

Se debe tener en cuenta que el manejo de la Historia Clínica en el caso específico del Instituto Nacional Materno Perinatal es manual, soportándose en un sistema de información implementado por el departamento de Estadística e Informática, el cual se utiliza principalmente para generar los números correlativos de Historia Clínica, la recolección de información básica del usuario y la generación de citas y pre facturas de atención.

3.3 Política de Seguridad de la Información

Habiéndose establecido el alcance para el desarrollo del Sistema de Gestión de Seguridad de la Información, el establecimiento de una Política de Seguridad de la Información es de vital importancia dado que especifica los lineamientos generales de seguridad que deben ser cumplidos en la organización – los cuales deben ir alineados a los objetivos del negocio – además de los objetivos que se busca alcanzar respecto a la seguridad de la información en los ámbitos definidos en el alcance.

Dado que se debe asegurar su cumplimiento, la Política de Seguridad de la Información debe ser aprobada por la Alta Dirección que además tiene la obligación de comunicar en la institución la importancia que tiene para la misma el lograr alcanzar los objetivos trazados en la política.

La política de Seguridad de la Información propuesta para el presente caso de estudio es la siguiente:

> *"La atención en servicios de salud pública se soporta en sistemas de información basados en software o de manera manual que permiten gestionar la información de los pacientes.*
>
> *Como institución dedicada a la atención de pacientes en gestación y post-parto, el Instituto Nacional Materno Perinatal (INMP) tiene la obligación de proteger éstos sistemas y la información que los mismos almacenan o generan para brindar un servicio de calidad, de lo contrario un incidente que afecte a la información podría dificultar a algún modo el acto médico o tratamiento llegando incluso a generar daños a la salud tanto de la paciente como de su bebé.*
>
> *Adicionalmente es obligación del INMP garantizar la confidencialidad de los datos personales y sensibles de sus pacientes en todo uso que a éstos se les pueda dar, siguiendo los lineamientos otorgados por la ley y el uso ético de los mismos. Por este motivo se debe contar con el consentimiento del paciente previa comunicación del uso que se le dará a su información.*

Los colaboradores del INMP deberán ser comunicados de la presente política de seguridad entendiendo la responsabilidad que tienen de manera individual en cuanto a la confidencialidad, integridad y disponibilidad de la información.

De esta manera los colaboradores deben comprometerse con el cumplimiento de lo establecido por el presente documento, así como con las políticas y procedimientos relacionados – tanto los ya vigentes como los que se publiquen posteriormente, comunicando de acuerdo al esquema de escalamiento definido aquellos casos en los que se encuentre un incidente que contradiga lo establecido por este documento."

Como se mencionó en el anterior párrafo, es importante establecer los objetivos de seguridad de la información que sirvan como criterios a tener en cuenta en los siguientes pasos del análisis y diseño del SGSI. Los objetivos definidos para el presente caso son:

"Objetivos de seguridad de la información en el INMP

- *Ofrecer un servicio de calidad a las pacientes, garantizando que se apliquen los controles necesarios para asegurar su información.*
- *Cumplir con los requerimientos legales en cuanto a la protección de la información de los pacientes.*
- *Establecer y monitorear un Sistema de Gestión de Seguridad de la Información que identifique los riesgos a los que se expone la información en el INMP y pueda definir controles para los mismos.*
- *Concienciar al personal sobre la importancia del SGSI, así como su responsabilidad sobre el cumplimiento de lo dispuesto por el SGSI."*

4 CAPÍTULO 4: Mapa de procesos del alcance

4.1 Modelado de los procesos de negocio establecidos en el alcance del proyecto

En el presente capítulo se muestran los modelos – utilizando la notación BPMN 2.0 con el apoyo de la herramienta Bizagi Modeler – de los dos procesos establecidos en el alcance del proyecto.

Cabe destacar que dicho modelado de procesos no forma parte del conjunto de políticas y procedimientos que conforman el Sistema de Gestión de Seguridad de la Información, sin embargo son requeridos como información que alimenta el análisis realizado durante el diseño del SGSI, el cual es un sistema orientado a procesos.

En un caso ideal la institución sobre la que se realiza el proyecto debería contar con todos sus procesos documentados, sin embargo al no encontrarse esta información el equipo encargado de llevar a cabo las actividades se encuentra en la necesidad de realizar el levantamiento de información correspondiente para poder realizar el modelado de procesos con la finalidad de poder realizar un análisis de los riesgos de acuerdo a la situación real de la institución.

Al analizar los procesos de negocio presentados a continuación, se puede evidenciar que la información contenida en las Historias Clínicas de los pacientes son utilizadas en diferentes ambientes, saliendo continuamente del archivo hacia los consultorios, así como generándose copias – ya sean simples o legalizadas – para su entrega a los pacientes, apoderados o personal perteneciente a la policía o personal judicial que así lo requiera.

La responsabilidad principal por la seguridad de estos documentos es del personal del área de Archivo y Admisión – áreas que se encuentran en la misma locación física – área con la que se realizará la identificación de

activos de información y el análisis de riesgo necesarios para poder establecer los controles requeridos para garantizar la seguridad de la información en ambos procesos de negocio.

El detalle referente a los subprocesos que conforman parte de los diagramas presentados a continuación se puede encontrar en las secciones “Anexo 4: Subprocesos del Proceso de Admisión de Pacientes” y “Anexo 5: Subprocesos del Proceso de Emisión de copia de Historia Clínica” en el documento de anexos que acompaña al presente proyecto.

Mapa del Proceso Principal de Admisión de Pacientes

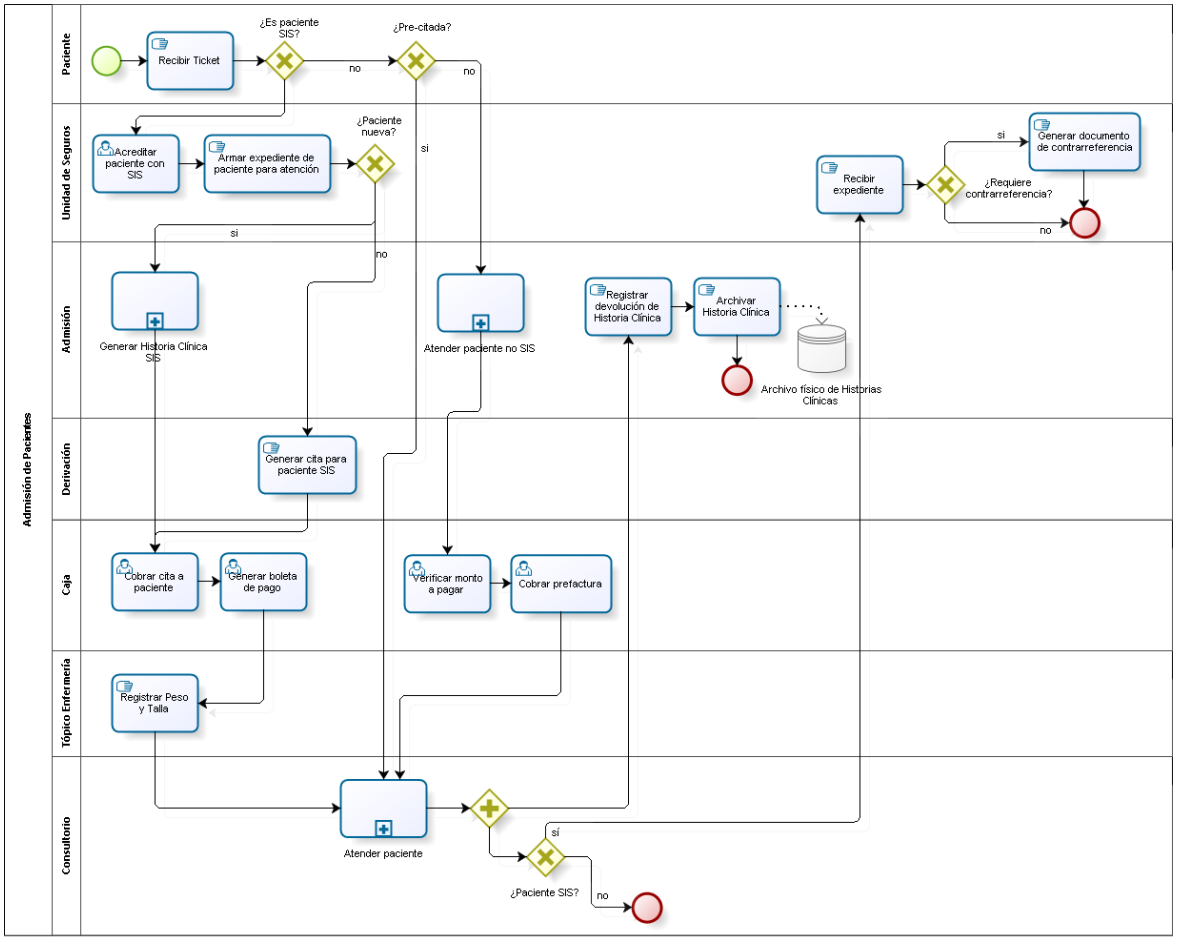

Ilustración 5 Proceso de negocio de Admisión de Pacientes Fuente: Elaboración propia

Mapa del Proceso Principal Emisión de Copia de Historia Clínica

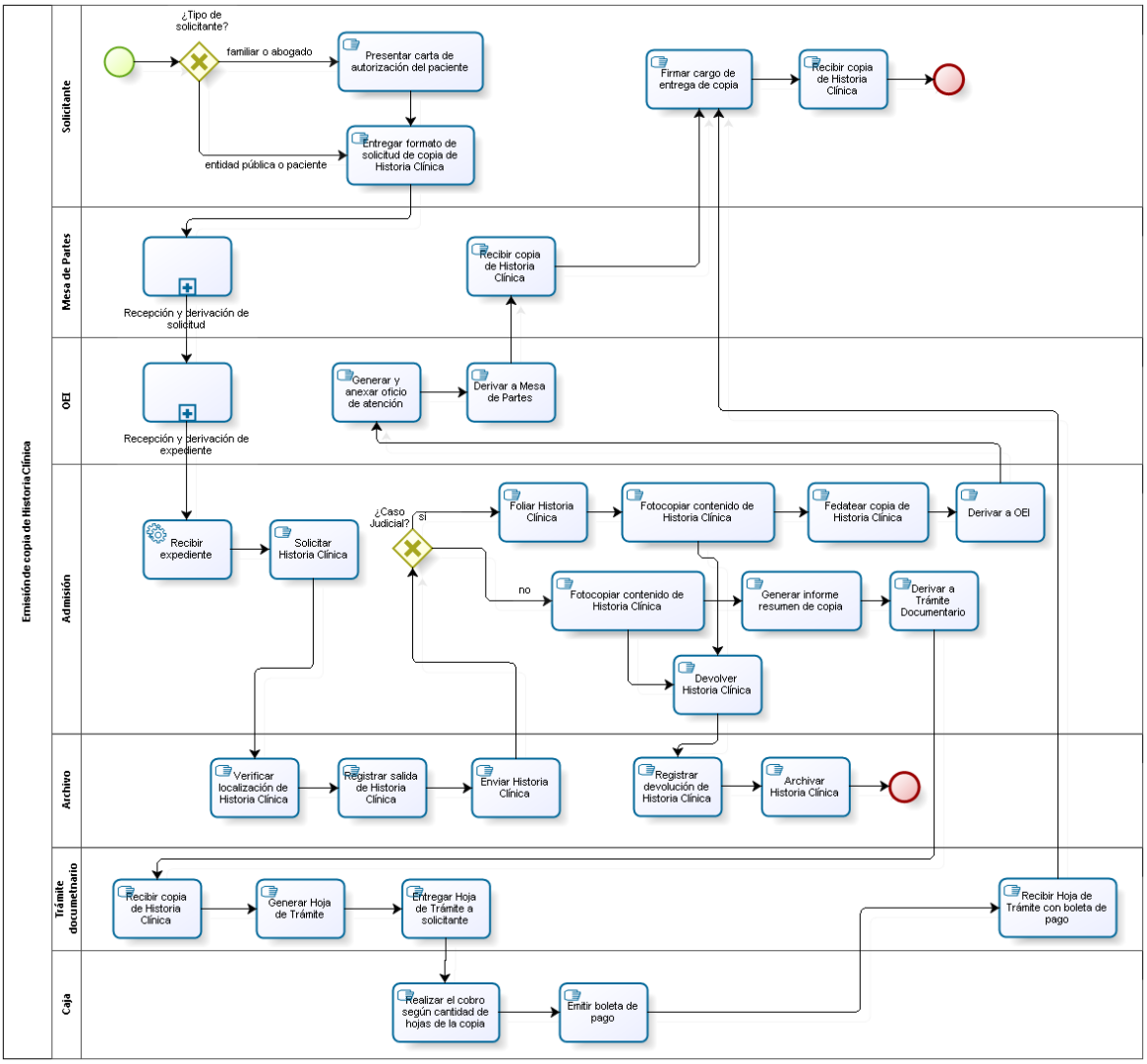

Ilustración 6 Proceso de negocio de Emisión de Copia de Historia Clínica Fuente: Elaboración propia

5 CAPÍTULO 5: Metodología de Análisis de Riesgos

El análisis de los riesgos de seguridad de la información presentes en los procesos de negocio pertenecientes al alcance escogido para el análisis es una etapa fundamental en el desarrollo del SGSI. Este proceso establece la metodología que se utilizará para definir los criterios de aceptación y valoración de los riesgos de seguridad de la información, además de la identificación, análisis y evaluación de los mismos sirviendo como entrada directa para el proceso de determinación de los controles aplicables al escenario presentado.

La metodología de riesgos presentada a continuación utiliza el estándar ISO/FDIS 31000:2009 la cual brinda principios genéricos para la gestión del riesgo que deben ser contextualizados en base a las particularidades encontradas en el INMP y al alcance escogido.

La gestión de riesgos en el INMP es requerido para el cumplimiento de la implementación de un SGSI que sea efectivo en el control de la información que se transmite a través de los procesos de negocio de la institución, siendo responsabilidad de la entidad institucional creada con la finalidad de mantener la gestión de la seguridad de la información – siguiendo los lineamientos de la implementación de la NTP 27001:2008 esta entidad debería ser constituida como “Comité de Seguridad de la Información” – teniendo además la responsabilidad de realizar un seguimiento de los riesgos y controles establecidos como parte del sistema de seguridad dado que los cambios de diferentes factores – organizacionales, creación de nuevos servicios, cambios de personas, etc. – pueden modificar el análisis de los riesgos, pudiendo incluso llegar a hacer que los controles en funcionamiento no sean los adecuados.

Para la clasificación y valoración de los riesgos, en el presente proyecto se ha optado por definir una matriz de calor que considere la probabilidad de que una amenaza explote una vulnerabilidad y el impacto que dicho evento – o sus consecuencias – puedan tener sobre el negocio. La categorización de ambos criterios es la siguiente:

Criterio de probabilidad

Rara	Poco probable	Posible	Muy probable	Casi certeza
Frecuencia de ocurrencia muy baja, o probabilidad muy remota de ocurrencia.	Frecuencia de ocurrencia baja (un evento cada 2 a 5 años).	Frecuencia de ocurrencia media (un evento cada 1 a 2 años).	Frecuencia de ocurrencia bimensual.	Frecuencia de ocurrencia mensual, certeza muy alta de que ocurrirá dicho evento.

Tabla 3 Criterios de probabilidad utilizados en el proyecto Fuente: Elaboración propia

Para el uso de la presente categorización, se deberá tener en cuenta la probabilidad de ocurrencia, teniendo como guía el tiempo que ejemplifica a cada una de las clases establecidas.

Criterio de impacto

Muy Bajo	Bajo	Medio	Alto	Muy Alto
La información afectada es de dominio público o con una baja importancia, como por ejemplo las citas generadas, o las recetas médicas.	La información afectada tiene un impacto bajo en la atención del paciente, afectando el tiempo de atención del mismo pero no limitándolo.	La información afectada afecta la atención de los pacientes, paralizando el servicio por máximo 1 día.	La información afectada impacta en un nivel alto el servicio, paralizándolo por una semana. Incluye también la filtración o pérdida de información personal.	La información afectada impacta al servicio inhabilitándolo por más de una semana. Incluye además la filtración o pérdida de información sensible.

Tabla 4 Criterios de impacto utilizados en el proyecto Fuente: Elaboración propia

Para el uso del presente criterio, se deberá tener en cuenta qué tanto afecta las operaciones del servicio la materialización de una amenaza, además de la información que pueda verse comprometida como consecuencia de la misma.

Matriz de calor

Los criterios que se han definido se utilizan en conjunto para conformar la matriz de calor sobre la que se realizará la valoración de los riesgos identificados en el análisis. A continuación se presenta la matriz de calor generada en base a dichos criterios.

Probabilidad de materialización		Nivel de Impacto				
		Muy bajo	Bajo	Medio	Alto	Muy Alto
		1	2	3	4	5
Casi certeza	5	Moderado	Alto	Alto	Extremo	Extremo
Muy probable	4	Bajo	Moderado	Alto	Alto	Extremo
Posible	3	Bajo	Moderado	Moderado	Alto	Alto
Poco probable	2	Bajo	Bajo	Moderado	Moderado	Moderado
Rara	1	Bajo	Bajo	Bajo	Bajo	Moderado

Tabla 5 Matriz de calor utilizado para la valoración de riesgos identificados en el proyecto Fuente: Elaboración propia

Apetito por el riesgo

Se denomina “apetito por el riesgo” al nivel de riesgo que una empresa está dispuesta a aceptar, sin necesidad de realizar un análisis extenso de los mismos, ni establecer controles que los mitiguen, dado que se considera que su impacto es bajo en relación a los procesos de negocio. En empresas que recién inician la implementación de controles para los riesgos que posean, lo normal es que el apetito por el riesgo sea de un nivel Bajo, centrándose en controlar aquellos riesgos de nivel Moderado, Alto y Crítico. Dado que el INMP posee algunos controles ya establecidos para el control de riesgos, se considerará un apetito por el riesgo similar.

Riesgo Residual

En el proceso de gestión del riesgo es importante que se tenga presente que los controles que se establezcan como producto del análisis no necesariamente mitigarán completamente el riesgo. Lo usual es que haya cierto nivel de riesgo que se mantenga presente luego de la aplicación de los controles, al cual se denomina Riesgo Residual y que debería ser de igual nivel al que se definió como apetito por el riesgo.

6 CAPÍTULO 6: Metodología de Valoración de Activos

Una vez establecida la metodología con la cual se realice el análisis de los riesgos que se identifiquen en los procesos de negocio del alcance del proyecto, es imperativo que se establezca una metodología con la cual se realice un estudio de los activos de información – definidos como algo que tiene valor o utilidad para la organización y que debe ser protegido – que participan en los mismos con la finalidad de contar con un inventario de activos y una medida de su valor para el negocio.

Con el apoyo de esta metodología se podrá determinar el valor que tienen dichos activos de información para la empresa, como entes de soporte, o transmisión de información y que podrían afectar alguno de los pilares de la seguridad de la información – Confidencialidad, Integridad y Disponibilidad – como consecuencia de la materialización de un riesgo que los afecte.

Identificación de activos

El proceso de identificación de los activos de información se debe realizar en conjunto con el personal que cuente con el mayor conocimiento de los procesos de negocio del alcance, así como de los recursos que éstos requieren para realizar sus funciones. Es una buena práctica que se establezca una escala cuantitativa que mida el nivel en que una pérdida o falla en el activo motivo del estudio afecte alguno de los pilares previamente descritos.

Según la clasificación que se encuentra en la norma ISO 17799:2005 se observa que la clasificación de los activos de información pueden ser de los siguientes tipos: datos, documentos impresos, software, activos físicos como computadoras o archivos de documentos físicos y personal. Sin embargo, el caso específico del Instituto Nacional Materno Perinatal, entidad prestadora de

servicios de salud, requiere que se tenga en cuenta algunas consideraciones especiales que se alineen a las necesidades de este tipo de entidades. De este modo se tendrá en cuenta lo recomendado en la ISO 27799:2008 que aplica el Código de buenas prácticas establecido por la ISO/IEC 27002 sobre el escenario de entidades dedicadas a brindar servicios de este tipo.

El manejo de la información personal relacionada con la salud es de alta importancia en el análisis para el diseño de un SGSI, de esta manera la metodología asociada al reconocimiento de éstos activos de información debe realizarse teniendo en cuenta que estas entidades deben cumplir con:

1. La responsabilidad – legal y ética – que se tiene sobre los activos de información de salud.

2. El establecimiento de personal dedicado a la custodia de éste tipo de información.

3. Establecer reglas documentadas para el uso aceptable de la información de salud. Sobre éste último punto se determinan varias directivas en la Norma técnica de Historias Clínicas (MINSA, 2005) y en la Ley de Protección de Datos Personales (CONGRESO DE LA REPÚBLICA, 2011).

Utilizando como base el modelado de los procesos de negocio realizado y con el apoyo del personal asignado como “dueños” de los procesos de negocio, se debe proceder a realizar la identificación de los activos de información utilizados así como la clasificación según las siguientes categorías:

1. Activos Primordiales, definidos como todos aquellos que participan directamente en el flujo de información de los procesos del alcance y que contienen información.

2. Activos no Primordiales o de Soporte al Flujo de Negocio, incluye aquellos activos que se utilizan como apoyo a los Primordiales en el flujo de negocio.

Se debe tener en cuenta durante el proceso de identificación de activos de información que estos no son exclusivamente sistemas de información o información digitalizada, para el presente caso de estudio se considera activo

de información – y cabe destacar que sería el más crítico – el documento denominado Historia Clínica.

Valorización de Activos

Como siguiente paso en la metodología después de haber identificado los activos que participan en los procesos de negocio se debe realizar una valoración de los mismos de manera que se establezca aquellos que tienen una mayor importancia y, por ende, deben ser protegidos.

Como se definió en párrafos anteriores el criterio más adecuado a utilizar con este fin es un análisis de cuánto afectaría un incidente que ocasione la pérdida o falla de los activos identificados en base a los tres pilares de la Seguridad de la Información utilizando una escala de Likert (donde 1 es “muy poco” y 4 es “muy alto”).

El valor promedio de las tres medidas realizadas para cada activo de información determinará el valor de impacto general del activo, estableciendo su criticidad para el estudio realizado. En el presente análisis se ha definido que aquellos activos con un valor promedio de impacto mayor o igual a 3, son sobre los que se debe realizar el análisis de riesgos asociados, buscando establecer controles que los protejan de las amenazas presentes, asegurando la información que contienen o trasmiten.

En el desarrollo del análisis para el diseño del SGSI para el Instituto Nacional Materno Perinatal, se utilizará la siguiente tabla como formato del inventario de activos de información.

Modelo de Matriz de inventario de Activos de Información

Nro. Activo	Proceso de Negocio Asociado	Nombre del Activo	Descripción del Activo	Clasificación del Activo	Propietario del Activo	Valoración parcial			Valoración Final
						C	I	A	
ACT001	Admisión de pacientes	Sistema de Gestión Hospitalario	Utilizado para la gestión de citas y generación de número de Historia Clínica.	Activo Primordial	Admisión	4	3	4	4
ACT002	Admisión de pacientes	Archivo físico de Historias Clínicas	Archivo activo de Historias Clínicas, que contiene aquellas que pueden ser requeridas más frecuentemente.	Activo Primordial	Archivo	4	4	4	4
ACT003	Admisión de pacientes	Boleta de atención	Documento que detalla la información para realizar el pago de la cita por parte de la paciente.	Activo no Primordial	Paciente	1	1	1	1
ACT004	Admisión de pacientes	Cita médica	Documento exclusivo que presenta el paciente como comprobante de su atención programada consultorios externos.	Activo no Primordial	Paciente	1	2	2	2

Tabla 6 Modelo de Matriz de inventario de Activos de Información Fuente: Elaboración propia

Escala de valoración de Activos de Información

Valor en escala Likert	Pilares de Seguridad de la Información		
	Confidencialidad	Integridad	Disponibilidad
1	La publicación o filtración de la información no presenta un riesgo para la organización. Se puede considerar como información de dominio público.	Si la información presentada en el activo no es correcta o tiene un porcentaje de error del 25% no presenta un riesgo para la organización dado que no afecta de manera crítica las actividades de la misma.	En caso se requiera el activo de información debe poder ser accesible un 25% de las ocasiones en que se haga necesario, sin embargo su no disponibilidad por distintos factores no se considera un riesgo.
2	El activo de información debería ser sólo de uso interno a la organización, sin embargo su filtración no supone un riesgo o un daño para la misma.	Se requiere que el activo tenga un porcentaje de error como máximo del 50%, dado que un porcentaje mayor podría perjudicar a la organización.	El activo de información debe ser accesible el 50% de las veces en que se requiera, caso contrario podría perjudicar de manera leve a la organización.
3	El activo de información contiene información de índole privada, debiendo establecer controles para el acceso al mismo. Su filtración supone un riesgo moderado para la organización.	El activo de información debe contener información correcta en un 75%, caso contrario se podría generar un daño moderado a la organización o incluso iniciar acciones legales contra la misma.	Se requiere que sea accesible el 75% de las ocasiones en que se necesite, de lo contrario se perjudica moderadamente los procesos de negocio asociados al mismo pudiendo conllevar a consecuencias legales.
4	La información contenida por el activo es altamente sensible y debe ser protegida contra cualquier posible filtración, caso contrario los dueños de la información contenida pueden ser afectados y la organización ser demandada o multada.	La información no debe contener errores, de otro modo se afecta seriamente los procesos de negocio asociados, siendo susceptible la organización a ser demandada o multada.	La información contenida en el activo de información no puede ser inaccesible dada su criticidad. Su no disponibilidad se traduce en una paralización de las actividades asociadas ocasionando pérdidas serias o acciones legales en contra de la organización.

Tabla 7 Escala de valoración de Activos de Información Fuente: Elaboración propia

7 CAPÍTULO 7: Mapa de Riesgos

Luego de documentar la Metodología de Análisis de Riesgos y Valoración de Activos, ambos documentos serán puestos en práctica durante el análisis realizado que tiene por objetivo establecer el Mapa de Riesgos identificados.

De esta forma se procedió a realizar un inventario de los Activos de Información involucrados en ambos procesos de negocio con el apoyo del personal que labora en el área de Admisión y Consultorios Externos. Dichos activos serán valuados según el impacto que pueda producirse en los diferentes pilares de seguridad, tal y como se definió en la metodología correspondiente, identificando aquellos activos de información críticos para los procesos de negocio.

A continuación se pondrá en marcha el análisis de los riesgos a los que se encuentran expuestos los activos de información críticos, estableciendo de acuerdo a la metodología de análisis de riesgos una valoración basada en la probabilidad de ocurrencia y el impacto que pueda tener un incidente que afecte a dicho activo, siguiendo lo establecido en la metodología ya definida.

Finalmente se podrá establecer la estrategia a utilizar según el apetito de la empresa y de las posibilidades de la misma.

7.1 Inventario de activos

Haciendo uso del mapa de procesos previamente desarrollado, se realiza un análisis de los activos de información que se utilizan a lo largo del desarrollo de las actividades de los mismos. Este levantamiento de información se realiza con el apoyo de los denominados dueños de los procesos, quienes

participan continuamente en los mismos como parte de la operación de la institución.

Luego de establecer los activos de información identificados se procede a realizar una clasificación de los mismos, determinando el propietario del activo, la valoración del impacto en los tres pilares de Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad) y la valoración final del activo según el impacto que genera la pérdida o daño del mismo al proceso de negocio siguiendo la Metodología de Valoración de Activos diseñada para el proyecto.

El inventario de activos del presente proyecto se puede revisar en la sección "Anexo 6: Inventario de Activos de Información" en el documento de anexos que acompaña al presente proyecto.

7.2 Identificación y análisis de riesgos

Luego de haber realizado la identificación de los activos, así como su valoración para determinar su criticidad, se procede a realizar el análisis de riesgos sobre las actividades que se identificaron en el modelado de procesos del alcance del proyecto.

Haciendo uso de la metodología de Análisis de Riesgos desarrollada en el Capítulo 5 del presente documento, se realiza una revisión de los riesgos a los que dichas actividades se encuentran expuestas, determinando los factores que originan el riesgo, sus consecuencias y la evaluación del mismo que nos permitirá definir si se procederá a tratar o se aceptará como parte del apetito del riesgo de la institución.

La matriz de riesgos desarrollada como parte del diseño del SGSI puede encontrarse en la sección "Anexo 7: Matriz de Riesgos" en el documento de anexos que acompaña al presente proyecto.

8 CAPÍTULO 8: Declaración de aplicabilidad

Luego de haber realizado el proceso de análisis de riesgos, en el cual se identificaron los activos de información críticos y los riesgos a los que se encuentran expuestos actualmente con la finalidad de determinar las estrategias a seguir para su mitigación.

Sin embargo, estas estrategias no definen explícitamente las acciones a realizar puesto que son generales. Es por este motivo que la norma ISO/IEC 27001:2013 exige que se desarrolle el documento denominado “Declaración de aplicabilidad” en el que se detalla la selección de los controles a implementarse para mitigar los riesgos identificados. Este documento debe presentar la selección de los controles presentados en el Anexo A de la norma, detallando qué controles ya se encuentran implementados, cuáles se debe implementar (detallando de manera general las pautas que se debe tener en cuenta en su implementación) y cuáles de ellos no se implementarán (detallando el motivo de su exclusión).

En la presente Declaración de aplicabilidad se presenta una explicación contextualizada de los controles presentados en la norma en relación a su aplicación a una institución prestadora de servicios de salud como el INMP. Para ello se ha hecho uso del detalle de los controles que se encuentra en la ISO/IEC 27002:2013 utilizando como apoyo adicional las consideraciones específicas para la implementación de dichos controles en entidades prestadoras de salud que ofrece la ISO/IEC 27799:2008.

La declaración de aplicabilidad desarrollada como entregable final del proyecto de diseño se encuentra en la sección “Anexo 8: Declaración de Aplicabilidad” en el documento de anexos que acompaña al presente proyecto

9 CAPÍTULO 9: Conclusiones y recomendaciones

En este capítulo final del presente proyecto se realizará la presentación de las distintas situaciones que se consideran importantes y han afectado el desarrollo de las actividades del mismo – ya sea de manera positiva como negativa.

A continuación se presentará las conclusiones a las que se ha llegado respecto al proceso de análisis y diseño de un SGSI para el Instituto Nacional Materno Perinatal para finalmente detallar las recomendaciones que podrán ser de gran apoyo al momento de realizar el diseño y la implementación del SGSI a escala institucional, así como incrementar los niveles de seguridad en diferentes aspectos según lo desarrollado en el presente documento.

9.1 Observaciones

Durante el desarrollo del proyecto de fin de carrera se pudo verificar el gran retraso en el proceso de implementación, en comparación con la programación establecida por la ONGEI para todas las instituciones públicas, del INMP en cuanto a la Norma Técnica Peruana NTP ISO/IEC 27001:2008. No se ha gestionado actualmente el proyecto de implementación a pesar de que el plazo final previo a la fase regulatoria venció en el presente año. Es notorio que el principal interés de la institución es realizar inversiones relacionados a los servicios de salud.

El área de Estadística e Informática, que sería el ente ideal para liderar el proyecto, no ha tenido una gestión adecuada en los últimos años, dado que la dirección de la misma se encontraba ocupada por médicos con

poco o nulo conocimiento en cuanto a temas tecnológicos, motivo por el cual no se ha contado con una dirección adecuada de dicha área.

La nueva directiva de la institución se encuentra interesada en realizar proyectos de mejora en diferentes frentes más allá del ámbito de salud que lleven a la misma a ofrecer un mejor servicio a sus pacientes, haciendo ideal la presentación de proyectos de mejora en el frente tecnológico de la institución.

En cuanto a cumplimiento regulatorio, es notoria la falta de conocimiento por parte del personal del área relacionada a la gestión de Historias Clínicas en cuanto a la nueva normativa que se debería tener en cuenta en las labores que se realicen con este activo de información, tal como la Ley de Protección de Datos Personales. La institución se encuentra sujeta a la Ley de Transparencia (CONGRESO DE LA REPÚBLICA, 2002), la cual en su Artículo 15°-B Inciso 5 establece un lineamiento general respecto a la protección de datos personales sin mayor especificación de los tipos de datos o consideraciones especiales a tener, tal y como lo especifica la norma anteriormente mencionada.

Es importante señalar que uno de los principales problemas que se tuvo que afrontar en la elaboración del proyecto fue la huelga médica durante la cual se detuvieron las labores de la institución, retrasando el levantamiento de información debido a la falta de disponibilidad de personal. Adicionalmente el cambio de la directiva también afectó en el levantamiento de la información, teniendo que presentarse nuevamente el proyecto a las autoridades que tomaron los cargos.

9.2 Conclusiones

Habiendo finalizado el análisis y diseño del SGSI, se ha podido llegar a las siguientes conclusiones:

Existe una brecha importante en cuanto a seguridad de la información en la institución sobre la que se ha realizado el presente proyecto. La principal falencia que debería ser resuelta cuanto antes es involucrar a la dirección en las acciones del plan que se debe definir con motivo de la implementación del SGSI institucional, el cual debería ser gestionado como un proyecto institucional, de manera que se cuente con el apoyo de las distintas direcciones y áreas del INMP.

Es de vital importancia que se defina formalmente el comité de Seguridad de la Información, órgano que debería encargarse del proyecto de implementación del SGSI y que deberá contar con el apoyo de la Dirección General de modo que se facilite el acceso a la información de todas las áreas pertinentes.

El factor humano que constituyen los colaboradores debe ser apropiadamente atacado en cuanto a los cambios que el proyecto. Esto deberá incluir sesiones de capacitación en las que se concientice al personal sobre la importancia de la información con la cual se realizan las labores institucionales, así como fomentar el cumplimiento de las políticas que garantice la seguridad de la misma.

Es probable que la implantación de las nuevas condiciones de empleo para los colaboradores antiguos sea recibida con rechazo dado que muchos de ellos se encuentran trabajando mucho tiempo en la institución y puedan percibir este cambio como una amenaza. Este posible obstáculo deberá ser debidamente manejado en conjunto con el área de recursos humanos.

El tipo de actividades que realiza a la institución, así como la normativa a la cual se encuentra sujeta en cuanto a la gestión de Historias Clínicas (MINSA, 2005), obliga a que la información recolectada de los pacientes o generada durante la atención sea almacenada en formato físico. Este escenario al cual se adiciona la falta de definición de los procesos de

negocio y la caótica presencia de personas externas a la institución – pacientes, familiares, estudiantes, entre otros – incrementa la probabilidad de pérdida o extracción de información. Es pertinente indicar que las medidas actuales de aseguramiento de estos documentos no cumplen con los mínimos necesarios tanto en acceso físico, como en protección frente a incidentes como incendios, inundaciones, daño por humedad, etc. Esto ha sido evidenciado en paralelo al presente trabajo en el Censo Nacional de Archivos Realizado el presente año (ARCHIVO GENERAL DE LA NACIÓN, 2014).

El SGSI se encuentra estrechamente relacionado con la gestión de riesgos de una institución y tal como se puede evidenciar en el presente documento, el análisis que realiza no está sesgado a los activos o controles tecnológicos que la institución pueda tener o requiera. Es por este motivo que el equipo que tenga la responsabilidad de mantener el SGSI debería trabajar en conjunto con el área de Control Interno apoyándose en el mismo durante el análisis de los riesgos de la institución dado que dicha área debería tener una visión holística de los riesgos que se presentan en la misma. De igual manera el monitoreo de los controles aplicados por el SGSI debería conformar una parte del trabajo que realiza el área de Control Interno, garantizando la aplicación de los mismos como parte del plan maestro institucional.

9.3 Recomendaciones y Trabajos futuros

Dado que en las empresas del sector público el cambio en el organigrama institucional así como la creación de nuevos cargos debe pasar un proceso de aprobación que se realiza ante autoridades superiores, se recomienda como medida temporal que se establezca un comité de seguridad liderado por la Jefatura de la Oficina de Estadística e Informática en conjunto con la Dirección General del INMP y que deberá incluir a las jefaturas de las diferentes unidades de la institución.

Sin embargo, se debería iniciar formalmente el proceso de solicitud correspondiente que permita la creación de un área de seguridad de la información que permita contar con personal especializado y dedicado al control y mantenimiento del SGSI, permitiendo poner en práctica lo desarrollado en el presente proyecto de fin de carrera.
En este proceso es de vital importancia para el éxito de la implementación que se defina el cargo del Oficial de Seguridad de la Información, el cual – en conjunto con el área de Seguridad de la Información – debería pertenecer a alguna de las direcciones institucionales o conformar una nueva, de modo que tenga un nivel de acción más alto que el de las demás direcciones y reporte directamente a la Dirección General del INMP. Esta localización en la estructura organizacional es necesaria puesto que el SGSI requiere que se garantice el cumplimiento de las políticas definidas, así como el apoyo de todas las áreas de la institución.

Es pertinente especificar que el proceso de implementación del SGSI, además de requerir un compromiso por parte de la Alta Dirección de la institución, así como de todo el personal de la misma para garantizar el cumplimiento requerido por el mismo, implica una inversión monetaria en personal capacitado, equipos y controles de seguridad. Por este motivo el proceso de implementación a nivel institucional debe ser realizado como parte de un proyecto mayor que sea desarrollado en fases similares a las que se han realizado en el desarrollo del presente proyecto.

Se debe capacitar al personal integrante del comité de modo que puedan conocer el SGSI, el proceso de implementación con sus distintas fases y que puedan hacer extensiva la importancia del mismo en sus áreas.

Se debe realizar un trabajo en conjunto con el área de Planeamiento Estratégico que permita contar con el mapa de procesos de negocio de todas las actividades que el INMP realiza, debidamente aprobado por las distintas áreas. Esto apoyará al equipo encargado de la implementación a poder realizar una adecuada identificación de activos de información y el análisis de riesgos correspondiente.

La existencia de un SGSI por sí solo se encuentra enfocada a la protección de la información crítica para la institución – ya sea según su impacto en la confidencialidad, integridad o disponibilidad – de modo que se eviten incidentes de seguridad que puedan ocasionar escenarios que afecten las actividades del INMP o generen un impacto reputacional o financiero.
De manera complementaria a la implementación del SGSI se recomienda que la institución realice la implementación de un Sistema de Gestión de Continuidad de Negocios, enfocado en establecer planes a seguir durante un escenario que afecte la operativa de la institución. Este sistema de gestión y el SGSI permitirán tener un mayor nivel de protección no sólo sobre la información si no sobre los procesos críticos de la institución, contando con planes de contingencia que aseguren su recuperación luego de ser afectados por un escenario de desastre o incidente interno.

La obligación normativa que especifica que las Historias Clínicas de los pacientes deben estar almacenadas en formato físico – dado que son documentos legales – no excluye que dichos documentos puedan ser digitalizados. Iniciar un proyecto de digitalización de estos documentos – enfocándose en el archivo activo de la institución – permitirá que se cuente con un respaldo de la información de las mismas que podría ser utilizado en las actividades asistenciales mas no en cuestiones legales.

Se recomienda realizar un trabajo de consultoría enfocado a la seguridad del archivo de Historias Clínicas – tanto el activo como el pasivo – que permita contar con recomendaciones profesionales en cuanto a las medidas que se deban implementar para proteger estos documentos de daños por diferentes factores.

El diseño desarrollado en el presente documento presenta la aplicación de estándares aplicados a un entorno de una institución del sector salud

específica, sin embargo esto no limita su replicación en otras entidades públicas que brinden servicios de salud.

Para lograr esto, es necesario contar con los modelos de los procesos de negocio de la nueva institución, además se debe realizar una revisión de la metodología de riesgos desarrollada puesto que para distintas entidades la misma puede variar dependiendo de su apetito por el riesgo, así como la forma en que perciben los riesgos existentes.

De igual manera el inventario de activos de información debería ser realizado nuevamente – pudiendo reconocerse activos similares o iguales a los encontrados en este estudio.

Finalmente se debe ajustar el análisis de riesgos aplicándolo a la realidad de la institución, de modo que se pueda desarrollar una lista de controles debidamente adecuada a la nueva entidad.

Como trabajos futuros se propone realizar un análisis actual y rediseño de la red institucional, que se enfoque a mejorar los aspectos de seguridad informática – algunos de los cuales han sido detallados en el último capítulo de este documento – así como la implementación de algunos de los controles definidos en la Declaración de Aplicabilidad. También se recomienda el desarrollo de un sistema de información que facilite la digitalización y manejo de la información contenida en las Historias Clínicas que almacena el INMP.

Referencias bibliográficas

ALEXANDER, A. G. (2007). *Diseño de un sistema de gestión de seguridad de información: Óptica ISO 27001:2005.* Bogotá: Alfaomega Colombiana.

ARCHIVO GENERAL DE LA NACIÓN. (2014). *II Censo Nacional de Archivos - Cédula Censal de Entidades Públicas.* Lima.

CNB - INDECOPI. (2008). *NTP-ISO/IEC 27001:2008. EDI Tecnología de la información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información. Requisitos.* Lima.

COLEGIO MÉDICO DEL PERÚ. (2007). *Código de Ética y Deontología.*

CONGRESO DE LA REPÚBLICA. (1997). *Ley 26842. Ley general de salud.* Lima.

CONGRESO DE LA REPÚBLICA. (2002). *Ley 27806. Ley de Transparencia y Acceso a la Información Pública.* Lima.

CONGRESO DE LA REPÚBLICA. (2011). *Ley 29733. Ley de protección de datos personales.* Lima.

FARN, K.-j., Hwang, J.-M., & Lin, S.-K. (2007). Study on Applying ISO/DIS 27799 to Healthcare Industry's ISMS. *WSEAS Transactions on Biology and Biomedicine, 4*(8), 103-117.

GIBSON, J. (2010). *Managing Risk in Information Systems.* Massachusetts: Jones & Bartlett Learning.

GIUDICE, O., Fauquex, J., Scotti, S., & Yelen, M. (3 de Agosto de 2011). Protección de los Datos Personales de la historia clínica en Argentina y Uruguay e IHE XDS. *Journal of health Informatics*, 81-86.

HITPASS, B. (2007). *BPM: Business Process Management Fundamentos y Conceptos de Implementación* (Segunda ed.). Santiago de Chile: BHH Ltda.

HUERTA, L. A. (5 de Julio de 2011). *Promulgan Ley de Protección de Datos Personales (Ley Nº 29733)*. Recuperado el 6 de Junio de 2013, de Temas de derechos fundamentales: http://blog.pucp.edu.pe/item/137301/promulgan-ley-de-proteccion-de-datos-personales-ley-n-29733

INFORMATION COMMISIONER'S OFFICE. (29 de Noviembre de 2011). *The Guide to Data Protection.* Recuperado el 7 de Abril de 2013, de Data Protection and Freedom of Information advice - ICO: http://ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.ashx

INMP. (2012). *Plan Estratégico Institucional Multianual 2012-2016.*

ISACA. (2012). *CISM – Certified Information Security Manager – Review Manual 2013.* ISACA.

ISO 27001. (2013). *ISO 27001:2013. Information technology – Security techniques – Information Security management systems - Requirements.*

ISO 27002. (2013). *ISO 27002:2013. Information technology – Security techniques – Code of practice for information security control.*

ISO 27799. (2008). *ISO 27799:2008. Health Informatics – Information security management in health using ISO/IEC 27002.*

ISO 31000. (2013). *ISO 31000:2009. Risk management – Principles and guidelines.*

LEGISLATURA BI-CAMERAL JAPONESA. (2005). *Act on the Protection of Personal Information.* Tokio.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.* Madrid.

MINSA. (2005). *N.T. N° 022-MINSA/DGSP-V.02. Norma técnica de la historia clínica de los establecimientos del sector salud.*

MINSA. (2006). *R.M. 520-2006/MINSA. Lineamientos de política de seguridad de la información del Ministerio de Salud.* Lima.

ORMELLA, C. (Marzo de 2013). *Normas ISO de Seguridad de la Información.* Recuperado el 30 de Mayo de 2013, de Criptored - Red temática de criptografía y seguridad de la información: http://www.criptored.upm.es/guiateoria/gt_m327a.htm

PASSENHEIM, O. (2010). *Enterprise Risk Management* (Primera ed.). Ventus Publishing ApS.

PELTIER, T. R. (2005). *Information Security Fundamentals.* Florida: CRC Press.

PODER EJECUTIVO. (1991). *Código Penal Peruano.*

PRESIDENCIA DEL CONSEJO DE MINISTROS. (2012). *R.M. 129-2012/PCM. Aprobación del uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información. Requisitos".* Lima.

SHONIREGUN, C., Dube, K., & Mtenzi, F. (2010). *Electronic Healthcare Information Security.* Londres: Springer Science+Business Media.

TALABIS, M., & Martin, J. (2012). *Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data* (Primera ed.). Massachusetts: Elsevier Science.

UNITED STATES CONGRESS. (1996). *Health Insurance Portability and Accountability Act - HIPAA.*