PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA SERVICIOS POSTALES DEL PERÚ S.A.

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

David Arturo Aguirre Mollehuanca

ASESOR: Moisés Antonio Villena Aguilar

Lima, octubre de 2014

Resumen

La exigencia de la implementación de la norma técnica peruana NTP-ISO/IEC 27001:2008 en las entidades públicas nace de la necesidad de gestionar adecuadamente la seguridad de la información en cada una de estas empresas. Sin embargo, el desconocimiento de estos temas por parte de la alta dirección, ha ocasionado que no se tomen las medidas necesarias para asegurar el éxito de este proyecto en el tiempo estimado por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), entidad responsable de apoyar a las entidades públicas durante el proceso de implementación de la norma.

Debido a ello, para la realización de este proyecto de fin de carrera, se decidió trabajar con una entidad pública como caso de estudio, a fin de diseñar un Sistema de Gestión de Seguridad de Información o SGSI que se acople a la normativa a la cual está sujeta la organización y que pueda, en un futuro, servir como referencia para la implementación del mismo.

En consecuencia, se realizaron varias reuniones con la alta dirección que permitieran definir el alcance y las políticas del SGSI en la organización enfocándose en los procesos institucionales críticos de dicha entidad, posteriormente se realizó una serie de entrevistas que permitieran identificar y valorar los activos críticos de la organización así como identificar y evaluar los riesgos a los cuales estos estaban sometidos.

Por último, se presenta un documento llamado Declaración de Aplicabilidad en el cual se indica que controles de la NTP ISO/IEC 17799:2007 se pueden implementar dentro de la organización basado en el trabajo realizado dentro de la organización.

FACULTAD DE
CIENCIAS E INGENIERÍA
ESPECIALIDAD DE
INGENIERÍA INFORMÁTICA

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO INFORMÁTICO

TÍTULO: **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA SERVICIOS POSTALES DEL PERÚ S.A.**

ÁREA: TECNOLOGÍAS DE INFORMACIÓN
PROPONENTE: Moisés Villena Aguilar
ASESOR: Moisés Villena Aguilar
ALUMNO: David Arturo Aguirre Mollehuanca
CÓDIGO: 20070483
TEMA N°: 533
FECHA: 02 de octubre de 2014

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
Facultad de Ciencias e Ingeniería
0 6 OCT. 2014
MIGUEL MEJIA PUENTE
DECANO

DESCRIPCIÓN

El actual marco legal que afecta a las entidades públicas exige a aquellas que pertenezcan al Sistema Nacional de Informática la implementación de un Sistema de Gestión de Seguridad de Información (SGSI) utilizando la norma técnica peruana ISO/IEC 27001:2008. Sin embargo, muchas de estas organizaciones han colocado a cargo del proyecto a personal poco capacitado en estos temas, esto sumado a que las organizaciones no tienen experiencia en este tipo de proyecto, lo cual ha provocado que muchas no se ajusten al cronograma definido para la implementación del mismo.
Bajo este contexto, se presenta como alternativa de solución al problema identificado, el diseño de un SGSI alineado a la normativa peruana vigente para cubrir las necesidades de los procesos institucionales críticos de una entidad pública, de tal forma, que el documento resultante sirva como referencia a la implementación de la norma NTP ISO/IEC 27001:2008 en dicha empresa.
En el presente documento, se presenta como caso de estudio a la empresa Servicios Postales del Perú (SERPOST) S.A, una entidad afectada por este cambio de regulación, la cual decidió implementar este sistema de gestión definiendo como alcance aquellos procesos críticos para la atención de los clientes empresariales de la organización.

OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de información para SERPOST según lo indicado por la NTP ISO/IEC 27001:2008 y la NTP ISO/IEC 17999:2007 de seguridad de información a fin de realizar un diseño que le permita cumplir con los requerimientos legales a los que la organización se vio expuesta.

OBJETIVOS ESPECÍFICOS

1. Elaborar la documentación exigida por la NTP ISO/IEC 27001
2. Elaborar la valoración de activos de información de la empresa.
3. Elaborar la evaluación de riesgos
4. Elaborar la lista de controles para mitigar los riesgos detectados

ALCANCE

El alcance del presente proyecto abarca los siguientes procesos de atención a clientes empresariales:

- Admisión
- Habilitado

Av. Universitaria 1801
San Miguel, Lima – Perú

Apartado Postal 1761
Lima 100 – Perú

Teléfono:
(511) 626 2000 Anexo 4801

- Clasificación
- Control de Cargos
- Digitalización

De igual forma, el alcance solo abarcará la sede central de la organización.

Máximo: 100 páginas

Av. Universitaria 1801
San Miguel, Lima – Perú

Apartado Postal 1761
Lima 100 – Perú

Teléfono:
(511) 626 2000 Anexo 4801

Dedicatoria

Quiero dedicar este proyecto de fin de carrera a mi familia y amigos, especialmente a mis modelos a seguir, mis padres Carmen y Teodosio, que con amor y comprensión siempre estuvieron ahí para guiarme y aconsejarme cada vez que lo necesité.
A mis hermanos y cómplices Daniel, Janet y July, quienes me enseñaron con su ejemplo que todo se puede si lo deseas y te esfuerzas para lograrlo.
A mi incondicional compañera y mejor amiga Angela, que con su increíble sonrisa me alentaba y animaba a culminar este proyecto.
Y por último a Dios y a mi madre Auxiliadora, porque siempre me acompañan, les debo todo lo que tengo y todo lo que soy.

Agradecimientos

Quiero agradecer muy especialmente al Ing. Moisés Villena, por su paciencia y asesoría, sin su apoyo no hubiera podido terminar exitosamente este proyecto.
A la Srta. Marina Marcovich, la Ing. Shirley Muñoz y al Ing. Justo Vásquez quienes decidieron confiar en mí y me brindaron las facilidades para la realización del proyecto.
Y a todas las personas que llegaron a mi vida, porque guardo las enseñanzas que alguna vez me dieron.

Índice

1. Capítulo 1: Generalidades

1.1. Problemática

La necesidad de gestionar la seguridad de la información nace de un entorno cada vez más globalizado donde las empresas deben tomar decisiones rápidas y eficientes convirtiendo la información en uno de los activos más importantes dentro de las organizaciones llegando a tener una importancia estratégica para muchas de ellas ya que les permite mantener una ventaja competitiva frente a otras empresas [NTP ISO/IEC 17799].

La seguridad de la información se encarga de la búsqueda de la preservación de la confidencialidad, integridad y disponibilidad de la información [NTP ISO/IEC 17799], es decir, buscar protegerla tanto de ataques físicos, tales como robos o incendios, como de ataques cibernéticos, tales como el aprovechar vulnerabilidades de los sistemas de información.

En nuestro país, desde hace más de diez años, las políticas del gobierno han ido recomendando una adecuada gestión de la seguridad de la información con resoluciones ministeriales tales como la N° 224-2004-PCM en la que aprueban el uso obligatorio de la NTP ISO/IEC 17799:2004 en las entidades públicas referente a las buenas prácticas para gestionar la seguridad de la información [NTP ISO/IEC 17799].

Adicionalmente, el marco legal de nuestro país obliga a las entidades públicas, pertenecientes al Sistema Nacional de Informática, el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basándose en la norma técnica peruana (NTP) – ISO/IEC 27001:2008 mediante la resolución ministerial N° 129-2012-PCM emitida en mayo del 2012.

Ambas normas técnicas peruanas, la NTP ISO/IEC 27001 y la NTP ISO/IEC 17799, están basadas en la familia de normas ISO 27000 correspondiente a seguridad de la información. La primera, es el estándar principal de esta familia y menciona cuales son los requerimientos para desarrollar un sistema de gestión de seguridad de la información basándose en el ciclo de DEMING, o ciclo Plan – Do – Check - Act, una metodología cíclica muy usada en las normas ISO relacionadas a normas de gestión [NTP ISO/IEC 27001].

Como parte de esta norma, se presenta el Anexo A – Objetivos de Control y Controles, en los cuales se propone una lista de 133 controles, divididos en 11 módulos, para resguardar los activos de información de posibles riesgos que se encuentren en la organización. La explicación en detalle de cada uno de estos controles se puede ubicar en la NTP ISO/IEC 17799:2007, ya que es la hermana de la primera y está basada en la ISO/IEC 27002:2005.

Los sistemas de gestión, son estructuras probadas para la gestión y mejora continua de políticas, procedimientos y procesos [BSI, 2013]. Este sistema, en particular, busca establecer, implementar y mejorar la seguridad de la información en una determinada organización [NTP ISO/IEC 27001], y deberá ser implementado según un cronograma propuesto por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), organismo encargado de apoyar a las entidades públicas durante el proceso de implementación de la norma, el cual, propone 5 fases para la implementación del SGSI, siendo muy similares a las fases propuestas en la norma técnica peruana, la cual a su vez se basa en el ciclo de DEMING.

La siguiente gráfica, véase figura 1.1.1, muestra un resumen del cronograma de implementación incremental de un SGSI en entidades públicas en comparación con el ciclo de DEMING, como se observa, las fases I y II de este cronograma están íntimamente relacionadas con la fase de Planeación de este ciclo, mientras que la fase III correspondiente al despliegue está ligada a la fase Do / Hacer, ya que se encarga de la implementación del SGSI en sí.

De igual forma, la fase de revisión, en ambos casos, hace referencia a la verificación de la correcta implementación y monitoreo del sistema, mientras que la fase de consolidación está ligada al último paso del ciclo de DEMING, ya que se encarga de implementar las mejoras y correcciones de lo detectado en la fase anterior.

Fase	Nombre	Objetivo	Relación con el círculo de Deming
I	ORGANIZACIÓN	Desarrollar actividades principales para la dirección e inicio de la implementación	PLANEAR - PLAN
II	PLANIFICACIÓN	Desarrollar las actividades de planificación requeridas por la norma	PLANEAR - PLAN
III	DESPLIEGUE	Implementación del SGSI	HACER - DO
IV	REVISIÓN	Evidenciar el cumplimiento de lo indicado por la norma	REVISAR - CHECK
V	CONSOLIDACIÓN	Auditar e implementar mejoras y correcciones al SGSI	ACTUAR - ACT

Figura 1.1.1 - Comparación entre el cronograma de implementación de la ONGEI y el círculo de Deming

Fuente: NTP ISO/IEC 27001:2008; Portal Oficial de la Oficina Nacional de Gobierno Electrónico e Informática http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552

La resolución ministerial se emitió a finales de mayo del 2012 y se hizo efectiva 45 días después de publicada en el diario “El Peruano” [RM-129-2012-PCM], en ella se mencionaban plazos máximos para cada fase tal como se puede observar en la figura 1.1.2.

Según este cronograma, las entidades públicas deben haber terminado la implementación de este sistema de gestión para finales de enero del 2014; sin embargo, se maneja muy poca información de los avances de las distintas entidades públicas con respecto a estos temas, siendo la ONP e INDECOPI las únicas del sector público con una certificación internacional relacionada a seguridad de la información [INDECOPI; 2013; Noticias]. Una de las posibles causas de esta situación es que la norma indica que se debe hacer, más no, como se debe hacer.

Fase	Nombre	Objetivo	Fecha Límite
I	ORGANIZACIÓN	Desarrollar actividades principales para la dirección e inicio de la implementación	Finales de Septiembre 2012
II	PLANIFICACIÓN	Desarrollar las actividades de planificación requeridas por la norma	Finales de Enero 2013
III	DESPLIEGUE	Implementación del SGSI	Finales de Enero 2014
IV	REVISIÓN	Evidenciar el cumplimiento de lo indicado por la norma	Finales de Mayo 2014
V	CONSOLIDACIÓN	Auditar e implementar mejoras y correcciones al SGSI	Finales de Septiembre 2014

Figura 1.1.2 - Plazos máximos para cumplir con la implementación del SGSI

Fuente: Portal Oficial de la Oficina Nacional de Gobierno Electrónico e Informática
http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552

En una entrevista realizada el 3 de mayo del 2013 al ingeniero Carlos Horna, entonces responsable del área de seguridad de la ONGEI, se pudo obtener algunos de los principales problemas que se está experimentando en la implementación incremental de la NTP – ISO / IEC 27001. [HORNA; 2013; Entrevista]

El principal problema que se ha encontrado es la colaboración de la alta dirección para el desarrollo del SGSI, por ejemplo, en el caso de la Presidencia de Concejo de Ministros (PCM) o la Presidencia de la Republica se necesitaría la posición firme del mismo presidente o del premier para poder llevar a cabo estas reuniones, algo complicado debido a la recargada agenda que poseen.

Otro de los puntos clave es el tema del plan de continuidad de negocio, el cual es contemplado en el desarrollo del SGSI. El contar con un plan de continuidad puede llegar a tomar mucho tiempo, entre el diseño y las pruebas necesarias para la aprobación del plan; de ahí la necesidad que cada entidad pueda delimitar correctamente el alcance de su SGSI, siendo uno de los puntos que la ONGEI enfatiza cuando alguna entidad le presenta su documento de alcance.

Por último, se tiene el tema del presupuesto, esto debido a que cada entidad posee un presupuesto limitado para el desarrollo del SGSI y se estima que en algunos casos la implementación de los controles puede exceder el presupuesto designado, especialmente si se trata de desarrollar un plan de contingencia, ya que los costos para contar con un centro alterno pueden llegar a ser muy altos [HORNA, 2013, Entrevista]. Debido a este punto es que en algunos casos no se puede contratar personal especializado para que cumpla las funciones de un oficial de seguridad de información, persona encargada de planificar y verificar el rendimiento de un SGSI [PELTIER; PELTIER; BACKLEY; 2005], siendo personal del área de TI los que deben asumir estos cargos e, incluso, en algunos casos no se puede adquirir los servicios de una consultoría para que los apoyen en la fase de análisis y diseño del SGSI, la cual es la base para la implementación del sistema.

Bajo este contexto, se presenta como alternativa de solución al problema identificado el diseño de un Sistema de Gestión de Seguridad de Información alienado a la normativa peruana vigente para cubrir las necesidades de los procesos institucionales

críticos de una entidad pública, para ello, debido a su pertenencia al Sistema Nacional de Informática, se eligió como caso de estudio la empresa "Servicios Postales del Perú S.A. – SERPOST" de tal forma, que el documento resultante sirva como referencia a la implementación de la norma NTP ISO/IEC 27001:2008 en esta empresa.

1.2. Objetivo general

Diseñar un sistema de gestión de seguridad de información para SERPOST según lo indicado por la NTP ISO/IEC 27001:2008 y la NTP-ISO/IEC 17999:2007 de seguridad de información.

1.3. Objetivos específicos

1. Elaborar la documentación exigida por la NTP ISO/IEC 27001

   Para iniciar con el diseño del SGSI, se deben desarrollar una serie de documentos que sirvan como marco de referencia de seguridad de la información para la organización, cada uno de los cuales será de utilidad para cumplir con la fase I del cronograma de implementación incremental propuesto por la ONGEI.

2. Elaborar la valoración de activos de información de la empresa.

   Se debe realizar una valoración de activos de información, para conocer aquellos activos que son importantes para la organización y puedan ser objeto de un análisis de riesgo según lo propuesto por la fase II del cronograma de implementación incremental propuesto por la ONGEI.

3. Elaborar la evaluación de riesgos

   Una vez identificados los activos valiosos para la organización, se deberá realizar un estudio para conocer los riesgos que representan una amenaza a estos, esto se ajusta a lo indicado por la fase II del cronograma de implementación incremental propuesto por la ONGEI.

4. Elaborar la lista de controles para mitigar los riesgos detectados

   Una vez se hayan identificado los riesgos, se deberá realizar una lista de controles a implementar en la organización, con este documento la organización estaría cerrando la fase II del cronograma de implementación incremental y podría empezar con la fase de DESPLIEGUE.

1.4. Resultados esperados

- Resultado 1 para el objetivo 1: Presentación del proyecto mediante un "*Business Case"*

A través del desarrollo de un "*Business Case"* buscamos obtener el apoyo de la alta dirección de la entidad pública para poder implementar adecuadamente este sistema de gestión.

- Resultado 2 para el objetivo 1: Alcance formal del SGSI.

Se debe definir el alcance del proyecto del SGSI ya que la NTP ISO/IEC 27001, la define como punto de partida para la correcta implementación del sistema de gestión. [ISO/IEC 27001:2005]

- Resultado 3 para el objetivo 1: Política de Seguridad de la Información

Se debe realizar una política de seguridad de la información que se acople a las políticas actuales y los objetivos estratégicos de la empresa y logre reflejar las expectativas de la organización en materia de seguridad. [PELTIER; PELTIER; BACKLEY; 2005]

- Resultado 1 para el objetivo 2: Mapa de procesos del alcance del SGSI

Se debe realizar un mapeo de los procesos que pertenecen al alcance del SGSI ya que permitirá conocer cuáles son los activos involucrados, los responsables, las entradas a los procesos y las salidas de cada uno de ellos.

- Resultado 2 para el objetivo 2: Metodología para valorar activos de información

Se necesita el desarrollo de una metodología que pueda ser adoptada por la entidad pública para valorar los activos de información, de esta forma, podremos identificar aquellas que son claves para la empresa.

- Resultado 1 para el objetivo 3: Desarrollo de una metodología de análisis de riesgos

Los riesgos son eventos que de ocurrir podrían amenazar los objetivos de una organización [NTP ISO/IEC 17799], por ello se necesita el desarrollo de una metodología que pueda ser adoptada por la entidad pública para evaluar el impacto de los riesgos que amenazan los activos críticos de información.

- Resultado 2 para el objetivo 3: Mapa de riesgos

El mapa de riesgos es una herramienta que permite realizar una adecuada administración de riesgos, es decir conocer a que riesgos está sujeto cada activo de información, cuál es la probabilidad que este riesgo se materialice y cuál es su impacto en caso suceda. [NTP ISO/IEC 17799]

- Resultado 1 para el objetivo 4: Listado de controles acorde a la norma NTP-ISO/IEC 17799

En este punto se utilizará los controles ubicados en la norma NTP ISO / IEC 27001 – Anexo A “Objetivos de Control y Controles”, los cuales son medios para mitigar los riesgos detectados y los que están por ser detectados. [NTP ISO/IEC 17799]

- Resultado 2 para el objetivo 4: Declaración de aplicabilidad

El listado de controles ubicados en el anexo A de la norma NTP ISO/IEC 27001 son explicados a mayor profundidad en la NTP ISO/IEC 17799 y es con esta norma que se puede elaborar la declaración de aplicabilidad, un documento formal que justifica por qué los controles escogidos pueden ser implementados dentro de la entidad pública o por qué no, según sea el caso.

1.5. Herramientas, métodos y procedimientos

1.5.1. Mapeo

En la tabla 1.5.1 se encuentra cada una de las herramientas a utilizar para alcanzar los resultados esperados del proyecto, se ha de aclarar que las metodologías utilizadas para este proyecto son:

- PMBOK 5ta edición, para la gestión del proyecto
- Ciclo de Deming, específicamente la fase de planeamiento, ya que es la metodología propia de la implementación del SGSI.

Resultados esperado	Herramientas a usarse
RE1 – OE1: Presentación del proyecto mediante un "*Business Case"*	ISO/IEC 27003
RE2 – OE1: Alcance formal del SGSI	NTP ISO/IEC 27001 e ISO/IEC 27003
RE3 – OE1: Política de Seguridad de la Información	ISO/IEC 27001 e ISO/IEC 27003
RE1 – OE2: Mapa de procesos del alcance del SGSI	**Business Process Modeling Notation o BPMN** (Notación para el Modelado de Procesos de Negocio) es una notación gráfica estandarizada que permite el modelado de procesos de negocio, en un formato de flujo de trabajo. **Bizagi Process Modeler** es un software de libre distribución que utiliza la notación estándar BPMN para el modelado de los procesos.
RE2 – OE2: Metodología para valorar activos de información	ISO/IEC 27003
RE1 – OE3: Desarrollo de una metodología de análisis de riesgos	ISO/IEC 27005 y la NTP ISO 31000
RE2 – OE3: Mapa de riesgos	ISO/IEC 27005 y la NTP ISO 31000
RE1 – OE4: Listado de controles acorde a la norma NTP-ISO/IEC 17799	NTP ISO/IEC 27001 – Anexo A
RE2 – OE4: Declaración de aplicabilidad	NTP ISO/IEC 17999

Tabla 1.5.1 - Mapeo de herramientas a utilizar

1.5.2. Herramientas

1.5.2.1. Business Process Model Notation – BPMN

El BPMN (o Notación para el modelado de procesos por sus siglas en ingles), es "un estándar que provee a una organización la capacidad de entender y comunicar entre sí los distintos procedimientos propios del negocio en una notación gráfica. De igual forma, permite conocer cuál es el rendimiento actual de la organización al trabajar con otras empresas". [OMG; 2013; traducido]

El objetivo principal de BPMN es el proporcionar un estándar para el modelado de procesos de la organización. Fue desarrollada por el BPMI (Business Process Management Initiative) que es parte de la OMG (Object Management Organization) desde que las 2 organizaciones se fusionaron en el 2005. Actualmente se encuentra en la versión 2.0 la cual fue emitida en marzo del 2011.

Como resultado se tienen los procesos de la organización en un BPD (Business Process Diagram) utilizando una técnica de diagrama de flujo muy similar al diagrama de actividades del estándar UML reduciendo así la brecha que existe entre el modelado de procesos y la implementación de los mismos.

Justificación: Al ser un estándar orientado al modelamiento de procesos, facilita el entendimiento de los procesos del negocio debido a su practicidad para ver los procesos en distintos niveles, diferenciando macro procesos de micro procesos, reduciendo la carga visual y facilitando la lectura del modelo.

El modelamiento de procesos dentro de un sistema de gestión de seguridad de información es vital, debido a que se deben conocer los procesos que están dentro de su alcance para asegurar el correcto levantamiento de activos de información y asignar los controles necesarios para asegurar la disponibilidad, integridad y confidencialidad de los mismos.

1.5.2.2. Bizagi Process Modeler

Es una solución informática de libre distribución desarrollada por la empresa Bizagi que permite diagramar y documentar los procesos de una organización de forma gratuita utilizando la notación BPM [Bizagi; 2013].

Adicionalmente permite exportar el trabajo a un archivo imagen PNG, JPG y BMP o a archivos Word o PDF; sin embargo, su mayor ventaja es el de ser de libre distribución.

Justificación: El proyecto está orientado a las necesidades de las entidades públicas, por lo que debemos evitar el uso de herramientas que necesiten el pago de licencias para no afectar el presupuesto designado, es por ello que, ante esta necesidad, se utilizará esta herramienta.

1.5.2.3. NTP ISO/IEC 27001:2008

Es la norma técnica peruana basada en el estándar internacional principal de la familia ISO 27000, correspondiente a las normas sobre seguridad de información [ISO/IEC 27000, 2012], y contiene, como su nombre lo indica, los requerimientos para desarrollar un Sistema de Gestión de Seguridad de Información.
Esta norma fue certificable hasta el año 2013; sin embargo, fue sustituida por la nueva versión de esta norma la ISO/IEC 27001:2013.

Entre los puntos que cubre esta norma internacional encontramos [ISO/IEC 27001:2005]:

- **Sistema de Gestión de Seguridad de Información**
  En este punto se busca es definir el alcance y las políticas del SGSI según las necesidades de la organización. De la misma manera, indica los pasos a seguir para identificar, analizar y evaluar los riesgos y sus posibles tratamientos.
  Obsérvese que este punto se enfoca en la planificación no solo del análisis, diseño e implementación del SGSI, sino también del mantenimiento y mejora del SGSI.

- **Responsabilidad de la gerencia**
  En esta norma se busca la participación activa de la alta dirección, ya que ellos son los dueños del negocio, la norma busca que ellos estén conscientes de las políticas de seguridad y de los planes del SGSI aprobándolos y dándoles a conocer ante toda la organización. De la misma manera, en caso se necesite más recursos son ellos los que lo proporcionaran.
- **Auditorías internas**
  La auditoría interna busca conocer si es que los puntos tratados con anterioridad por el SGSI siguen están operativos y actualizados y no se quedaron. Mediante este punto se busca comprometer a los gerentes de las diversas áreas de la empresa a asegurarse que las acciones se ejecuten según como fueron documentadas.
- **Revisión Gerencial del SGSI**
  Como se indicó, el SGSI busca la participación activa de la alta dirección, este punto se busca que el SGSI sea revisado al menos una vez al año por la alta dirección y así asegurar el correcto funcionamiento del mismo y mejorarlo en caso se detecten algunas oportunidades para hacerlo.
- **Mejora**
  El punto final contemplado por la norma, este se asegura de usar cada uno de los puntos anteriormente descritos para mejorar la efectividad del SGSI.
  La identificación de no conformidades en el SGSI, es decir, situaciones que no están acordes a nuestros planes o lo deseado por la organización terminaran en correcciones que permitirán mejorar nuestro SGSI.

Carlsom en el capítulo 2 del libro “Information Security Management Handbook, 6th edition” nos muestra 4 beneficios que posee la implementación de su norma hermana, la ISO/IEC 27001:2005, para mejorar la organización [2008, p. 17, traducido]:

1. **Seguridad:**
   La estructura propia de un SGSI muestra una clara dirección, las políticas son dadas por la alta dirección, los gerentes se encarga del cumplimiento y los detalles son sacados de la documentación generada. De esta manera se puede monitorear y evaluar los resultados de una forma más ordenada. El SGSI proporciona mayor seguridad si es que ha sido validado por un auditor externo brindando ventajas ya sea si somos consumidores o proveedores de información, después de todo trabajar con alguien que ha pasado exitosamente por esta auditoria asegura que no darán problemas de seguridad a la organización.
2. **Diferencia:**
   Un SGSI puede servir como un diferenciador de mercado mejorando la imagen que se proyecta. Muchos sectores demandan un cierto grado de confidencialidad al trabajar. Tener una certificación nos hace un socio estratégico para estas empresas.
3. **Permite negocios:**
   Al implementar un SGSI se busca cubrir el marco legal que afecta a la empresa y resguardar la información que se posea con ayuda de controles, sin embargo; este hecho también posibilita, a la empresa, el ingreso a otros mercados que exijan la gestión de seguridad de información tales como entidades financieras o que alberguen datos personales.
4. **Estructura:**
   Un SGSI brinda una estructura a la empresa, con una dirección y roles definidos, funciones y servicios delegados y métricas que pueden ser analizadas brinda una mejora continua a la empresa. En muchos casos, la implementación de un SGSI inspira a las organizaciones a tener un sistema de

gestión en otras áreas como recursos humanos, seguridad física continuidad de negocio, etc.

Justificación: El presente proyecto busca desarrollar un sistema gestión de seguridad de la información para una empresa pública y el presente ISO fue desarrollado para "proporcionar un modelo para implementar, operar, monitorear, revisar y mejorar un sistema de gestión de la seguridad de la información (SGSI)" [ISO/IEC 27001:2005].

Es por eso que se puede afirmar que esta es la norma base para el desarrollo del presente proyecto de fin de carrera, ya que en ella se encuentran los lineamientos necesarios para el diseño de un SGSI y así cumplir con lo solicitado con el primer y segundo resultado esperado.

1.5.2.4. NTP ISO/IEC 17799:2007

La norma técnica peruana ISO/IEC 17799:2007 fue elaborada por el Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI) utilizando como base la norma ISO/IEC 17799:2005 y solo cambiando terminologías propias del idioma español. [NTP ISO/IEC 17799:2007]

Sin embargo, desde el 1 de julio de 2007 la norma ISO/IEC 17799:2005 cambio de nombre a ISO/IEC 27002:2005, manteniendo su año de edición y sin alterar su contenido.

En esta norma ISO se explican de una forma más detallada cada uno de los controles y objetivos que se mostraron en el anexo A de la NTP ISO/IEC 27001.
Estos controles se pueden dividir en 11 dominios, 39 objetivos de control y 133 controles.

Los dominios se pueden observar en la figura 1.5.1 y son los siguientes [ISO/IEC 27002:2005]:

- **Políticas de seguridad**
  En este dominio se busca que la alta dirección demuestre su compromiso con el SGSI publicando y distribuyendo las políticas del SGSI previamente alineadas con los requisitos de la organización legales y operativos.

- **Aspectos organizativos para la seguridad**
  Busca gestionar la seguridad de la información dentro de la organización, de ser necesario se debería buscar el apoyo de consultores expertos en la seguridad de información, así mismo se busca asignar responsabilidades de seguridad en la organización y gestionar la seguridad de la información que es manejada por terceros o grupos externos.

- **Clasificación y control de activos**
  En este dominio se busca mantener una protección adecuada sobre cada activo de la organización, se recomienda asignar el custodio de los activos a sus dueños para que ellos sean responsables de sus confidencialidad, integridad y disponibilidad y clasificarlos para indicar el grado de protección que necesitan.

- **Seguridad en recursos humanos**
  Se busca asegurar que los empleados, contratistas y terceros que trabajan con la organización entiendan las responsabilidades que tienen al formar parte del SGSI y que estén capacitados para responder ante un evento o incidencia según sus roles.

- **Seguridad física y del entorno**
  En este dominio se trata de evitar cualquier tipo de acceso no autorizado a la organización o a sus distintas sub áreas, así como controlar el correcto funcionamiento de los equipos que envíen o reciban datos.

- **Gestión de comunicaciones y operaciones**
  Trata de gestionar el correcto uso de los equipo de comunicación así como de evitar cualquier tipo de ataque o malfuncionamiento de estos equipos que deriven en una pérdida o modificación de la información.

- **Control de accesos**
  Busca evitar que la información sea accedida o compartida por personal no autorizado en la organización y detectar actividades no autorizadas.

- **Adquisición, desarrollo y mantenimiento de sistemas**
  En este dominio se busca asegurar que los sistemas de información son seguros y cumplen con los requisitos de seguridad para evitar la pérdida, modificación o mal uso de los datos a través de los sistemas de información.

- **Gestión de incidentes en la seguridad de información**
  Busca asegurar que los eventos o incidencias relacionados a la seguridad de información sean comunicados de una manera eficiente para poder tomar acciones correctivas contra ellos a tiempo. Asimismo se busca tener claro que pasos seguir una vez se reciba la alerta de haber encontrado algún incidente.

- **Gestión de continuidad de negocio**
  Busca reaccionar con medidas correctivas frente a algún evento o incidencia que pueda detener parcial o completamente los procesos críticos del negocio contemplando la seguridad de la información. De esta forma se busca mitigar el efecto negativo que pueda tener este acontecimiento sobre la organización.

- **Cumplimiento**
  Este dominio busca evitar que se incumplan las normas o el marco legal bajo el cual se rige la organización. Este marco legal contempla las leyes que afectan a la empresa y al negocio, las obligaciones contractuales, requisitos reglamentarios y requisitos de seguridad. Pero también busca que los sistemas de información de la organización cumplan con las políticas de seguridad.

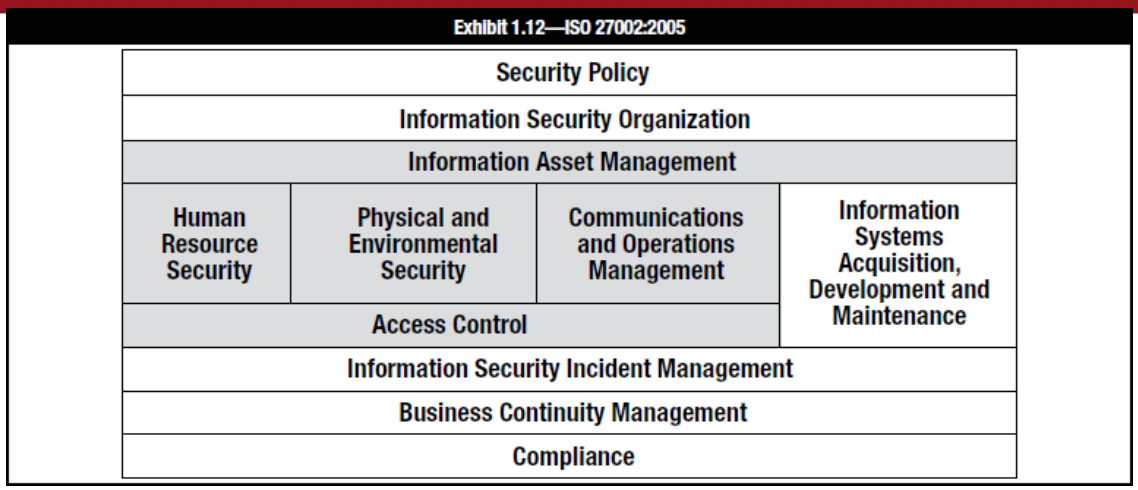

Figura 1.5.1 - Los dominios de la ISO/IEC 27002:2005

Fuente: Sacado del libro CISM Review Manual 2013

Justificación: Al estar basada en el anexo A de la NTP ISO/IEC 27001, contiene lineamientos prácticos para la implementación de los controles en la organización lo cual es de utilidad para el desarrollo del octavo resultado esperado que es la declaración de aplicabilidad.

1.5.2.5. ISO/IEC 27003:2010

El presente estándar brinda información y una guía práctica para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el diseño de un SGSI según lo establecido por la ISO/IEC 27001:2005.

La importancia del uso de este radica en que no cubre actividades propias del SGSI, solo muestra conceptos relacionados al diseño del plan del SGSI y lo que se debe realizar hasta antes de ejecutar el plan de implementación del sistema de gestión, lo cual está fuertemente vinculado al alcance del presente plan del proyecto.

Entre los puntos que aclara podemos encontrar los siguientes:

- Como preparar un plan de implementación de un SGSI para una organización
- Las actividades criticas del proyecto de un SGSI
- Ejemplos de cómo alcanzar los requerimientos de la ISO 27001

Como se mencionó, la presente norma ISO indica cómo debe realizarse el diseño del SGSI desde su inicio hasta el desarrollo de los planes de implementación, desde el proceso para obtener la aprobación de la alta dirección y la definición de un proyecto para la implementación del sistema de gestión, hasta la elaboración del plan final de implementación del SGSI.
Por último, como se menciona dentro del estándar, la ISO/IEC 27003 es aplicable a todas las organizaciones de todos los tamaños y tipos, considerando la complejidad y riesgos únicos de cada una de ellas. [ISO/IEC 27003:2010]

Justificación: Se decidió establecer como resultado esperado parte de la documentación propuesta por la presente norma, como es el caso del *Business Case,* debido a que brinda orientación para el desarrollo de un plan de implementación de un sistema de gestión de seguridad de la información cumpliendo con el alcance del presente proyecto al contemplar toda la documentación necesaria para el diseño de un

SGSI; sin embargo, también se incluye la ISO/IEC 27001 ya que esta es la norma base para el desarrollo del proyecto.

1.5.2.6. ISO/IEC 27005:2011

Hace uso del modelo de ciclo de Deming (PDCA) para gestionar los riesgos, es un estándar especializado que complementa a la norma internacional ISO/IEC 31000, la cual se especializa en la gestión de riesgos, indicando las mejores prácticas para gestionar los riesgos relacionados a la seguridad de la información. Se puede observar su proceso de gestión de riesgos en la figura 1.5.2

Existen varias metodologías para el análisis de riesgos, por ejemplo, tenemos a MAGERIT, una metodología de riesgos desarrollada en España que ayuda a identificar y planear un tratamiento de riesgos de las organizaciones [MAGERIT, 2012]. También existe OCTAVE, un conjunto de herramientas, técnicas y métodos para la valoración y planeamiento de la seguridad de la información basada en riesgos [OCTAVE].

Sin embargo, estas metodologías son más usadas en los contextos en las que fueron creadas. Por otro lado, la norma ISO/IEC 27005 es una norma internacional que complementa a la ISO/IEC 31000 y al ser parte de la familia ISO 27000 busca apoyar la tarea de análisis y gestión de riesgos a la hora de implementar el SGSI con el ISO/IEC 27001, es por este motivo que se adoptarán algunos aspectos de esta norma para el tratamiento de riesgos durante el proyecto.

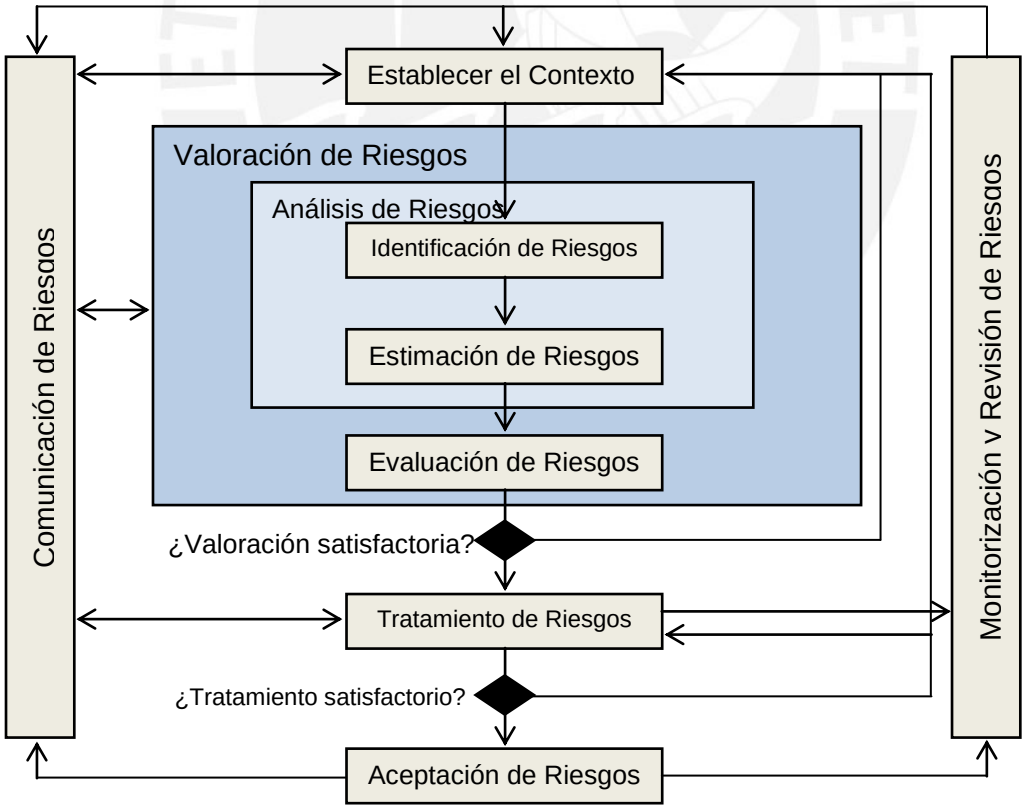

Figura 1.5.2 - Proceso de Gestión de Riesgos de Seguridad de Información

Fuente: Ilustración basada en el ISO/IEC 27005:2011

Justificación: Este estándar internacional nació para apoyar el análisis de riesgos al momento de implementar un SGSI. Adicionalmente, como se expuso en el estado del arte, es la metodología de riesgo recomendada por el ONGEI, es debido a estos motivos que utilizaremos esta norma para la gestión de riesgos junto a la NTP ISO 31000.

1.5.2.7. NTP ISO 31000:2011

Esta norma técnica peruana está basada en la ISO 31000:2009, la cual forma parte de la familia de estándares que gestionan el riesgo. Esto debido a la existencia de factores, internos o externos, que añaden incertidumbre en el logro de los objetivos de las organizaciones.

Esta norma busca establecer principios para tener una gestión eficaz del riesgo mediante la implementación y mejora continua de un marco de trabajo para la integración del proceso de gestión de riesgos en la planificación, estrategia, gestión, procesos de información, políticas, valores y cultura de la organización.

La gestión de riesgo se debe basar en:

- Crear valor
- Tratar la incertidumbre
- Formar parte de las decisiones
- Estar hecha a la medida
- Considerar factores humanos y culturales
- Facilitar la mejora continua de la organización

El proceso de gestión del riesgo lo podemos observar en la figura 1.5.3

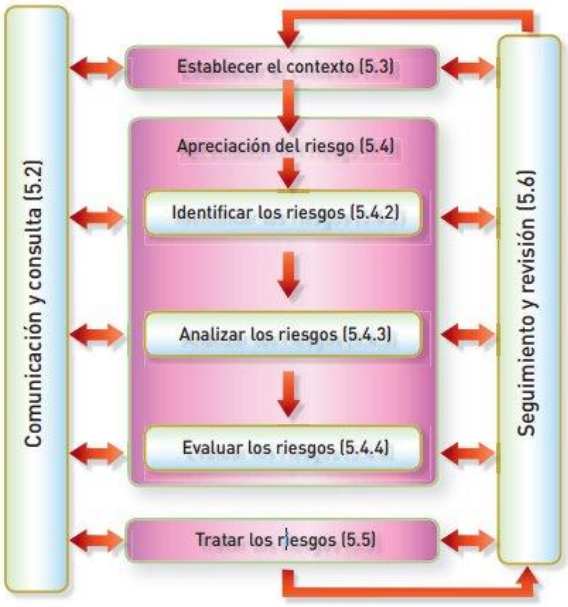

Figura 1.5.3 - Proceso de gestión de riesgos

Fuente: ESCORIAL, Ángel. 2012 "La gestión de riesgos impulsa la credibilidad y la transparencia". *Gerencia de Riesgos y Seguros.* España, No 112, p 51.

Justificación: Durante el análisis y valoración de riesgos, se utilizará esta norma debido a que es el estándar propuesto por el gobierno peruano para la gestión de riesgos [Resolución 007-2011/CNB-INDECOPI]

1.5.3. Metodologías

1.5.3.1. Guía PMBOK de PMI quinta edición

Justificación: La presente metodología será utilizada para la gestión del proyecto de fin de carrera, esto debido a que es aplicable a un amplio rango de proyectos y es un estándar adaptable para la gestión de estos.

PMBOK reconoce cinco procesos básicos que son los procesos de iniciación, planificación, ejecución, seguimiento y control y cierre; y 10 áreas de conocimiento de las cuales solo se usarán las siguientes [Project Management Institute; 2013]:

- **Gestión de la integración del proyecto**

Desarrollar el plan para la dirección del proyecto	Este punto será necesario ya que con él se detallaran cada una de las actividades que se realizaran como parte del proyecto.
Dirigir y gestionar el trabajo del proyecto	Este punto se verá reflejado en cada una de las actas de reunión que se tendrá con el asesor una vez se inicie el proyecto.
Monitorear y controlar el trabajo del proyecto	Esto se realizará con la revisión de los resultados esperados del proyecto.

- **Gestión del tiempo del proyecto**

Planificar la gestión del cronograma	El desarrollo del cronograma de trabajo es muy importante ya que nos ayuda a verificar si estamos cumpliendo con los tiempos definidos para la entrega puntual del proyecto y hacer las modificaciones necesarias en caso no lo estemos haciendo.
Definir las actividades	
Secuenciar las actividades	
Estimar la duración de las actividades	
Desarrollar el cronograma	
Controlar el cronograma	

- **Gestión de los interesados del proyecto**

Identificar a los interesados	En este punto solo se identificará cada una de las personas relevantes afectadas por el proyecto y su interacción con el mismo.
Gestionar el compromiso de los interesados	Estos puntos se verán reflejados en la carta de aceptación que emitirá la entidad pública para la realización del proyecto en ella. Es uno de los puntos necesarios para aclarar el alcance del proyecto y evitar mal entendidos en el desarrollo del mismo.
Controlar el compromiso de los interesados	

1.5.3.2. Ciclo de Deming - Ciclo PDCA

Justificación: La presente metodología posee los 4 pasos iterativos que pueden ser adaptados fácilmente a los sistemas de gestión siendo muy utilizado por las normas ISO de sistemas de gestión, incluyendo la de gestión de seguridad de información.

Conocido como círculo, rueda o ciclo de Deming o círculo o ciclo PDCA, por sus siglas en ingles Plan, Do, Check y Act. Se llama así debido a que nace a raíz de una conferencia que dio el Dr. W. Edwards Deming en Japón el año 1950.

La rueda de Deming se caracteriza por tener cinco (5) puntos clave, estos son [MOEN, NORMAN; 2009]:

1. Diseñar el producto con las pruebas apropiadas
2. Realizarlo probándolo en la línea de producción y en el laboratorio
3. Ponerlo en el mercado
4. Probar su utilidad y ver que piensa los usuarios de nuestro producto
5. Rediseñar el producto siguiendo los 4 pasos anteriores considerando la opinión de los usuarios.

Poco tiempo después esta rueda evolucionaria en el ciclo PDCA de la siguiente manera:

1. Diseñar – Planear (Plan): Diseñar el producto corresponde, en gestión, a la fase de planeamiento.
2. Producción – Hacer (Do): Este punto corresponde a la realización de lo que se ha planeado.
3. Venta – Verificar (Check): Ponerlo en el mercado corresponde a la fase de revisar que es lo que opinan los usuarios sobre lo que hemos realizado y si satisface sus necesidades.
4. Investigación – Actuar (Act): En caso de encontrar alguna queja debe ser incorporada en la fase de planificación y tomar medidas correctivas la próxima vez que se inicie este ciclo.

El uso del circulo de Deming es una práctica muy común en las normas ISO relacionadas a sistema de gestión, para el caso de un SGSI se puede adaptar según lo indicado en la figura 1.5.4.

Por ejemplo, Carlsom en el capítulo 2 del libro “Information Security Management Handbook, 6th edition” nos muestra los pasos para implementar el SGSI según el círculo de Deming [2008, p. 17, traducido]:

1. **Planear**: Establecer el SGSI
   Entender el contexto de la organización
   Evaluar los riesgos de la empresa
   Trazar programa de seguridad de información
   Evaluar los riesgos del programa

2. **Hacer**: Implementar y operar el SGSI
   Crear un plan base de seguridad de información
   Crear implementaciones específicas por cada dominio

3. **Verificar**: Monitorear y revisar el SGSI
   Evaluar el riesgo operacional

4. **Actuar**: Mantener y mejorar el SGSI
   Medir y monitorear

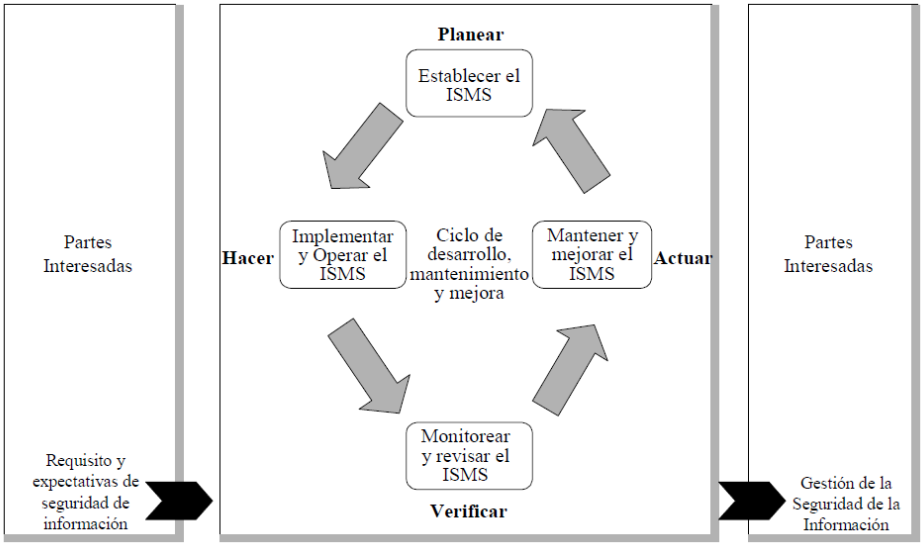

Figura 1.5.4 - Modelo PDCA aplicado al SGSI

Fuente: Sacado de la NTP ISO/IEC 27001:2008 – Tecnologías de información – Técnicas de seguridad – Sistemas de seguridad de la información - Requerimientos

De esta metodología solo se realizará el primer paso de “Planear” ya que el alcance del proyecto cubre el diseño más no la implementación, revisión ni mejora de un SGSI.

1.6. Alcance

El presente proyecto busca diseñar un sistema de gestión de seguridad de información para resguardar la confidencialidad, disponibilidad e integridad de los activos de información involucrados en los procesos institucionales críticos de una entidad pública. Debido a ello debemos considerar que el alcance del proyecto de fin de carrera estará claramente ligado al alcance que sea definido por la alta dirección de la empresa, siendo una base para definir el alcance del presente proyecto.

Por ello, luego de conversar con el oficial de seguridad de la información de la entidad donde se aplicará el diseño del sistema de gestión, se conoció que el alcance definido por la institución cubrirá todos los procesos relacionados a la atención de los clientes empresariales. Por consiguiente, se definió un alcance similar para el proyecto de fin de carrera.

Sin embargo, debido a que la empresa en la que se está realizando el diseño del SGSI tiene presencia nacional e internacional, se decidió, junto con el asesor, delimitar el alcance del SGSI a aquellos clientes que operan dentro de Lima.

Tampoco se contemplará el proceso de Facturación debido a que involucra procesos de otras áreas y maneja procesos muy complicados cuando se generan sanciones por incumplimiento de los plazos de entrega de paquetería.

Por último, debido a que la empresa posee 11 locales administrativos que también forman parte del proceso, se delimitará el alcance a un solo local, el cual será la sede principal de la empresa.

1.7. Limitaciones

- Para el desarrollo de un sistema de gestión de seguridad de la información se necesita el apoyo constante de la alta dirección, siendo una de las principales limitaciones que se tiene el compromiso y apoyo de estos debido a que se depende de su disponibilidad para aprobar los distintos documentos que nacen de los resultados esperados de este proyecto, tales como políticas de seguridad de información, modelamiento de procesos, alcance del sistema, metodologías, etc.

- Adicionalmente, se debe considerar que se está trabajando con una entidad del estado por lo que el SGSI debe estar acoplado a la normatividad a la que está sometida la entidad.

1.8. Riesgos

Los riesgos identificados en el proyecto se presentan en la tabla 1.8.1

Riesgo identificado	Impacto en el proyecto	Medidas correctivas para mitigar
Demora en la entrega de información necesaria.	En caso no se pueda acceder a la información necesaria para llevar a cabo el proyecto a tiempo incrementaría la duración del proyecto obligando a avanzar más rápido otros aspectos.	Se firmará una carta de aceptación con la entidad pública donde se realizará el proyecto para certificar su apoyo durante el mismo, en caso no se pueda acceder a tiempo a la información se buscará trabajar con una empresa pública alterna.
Negación de acceso a la información requerida.	Si no se puede acceder a la información de la empresa no se podrá realizar el proyecto de fin de carrera ya que no conoceríamos la situación actual de la empresa ni los activos a resguardar.	Se firmará una carta de confidencialidad para asegurar a la empresa que su nombre no será revelado, de igual forma se firmará una carta de aceptación para certificar su apoyo durante el desarrollo del proyecto. Por último, en caso la entidad pública decida no brindar la información necesaria se buscará trabajar con una entidad pública alterna.
Modificación del alcance o políticas de seguridad por parte de la alta dirección.	En caso la alta dirección decida cambiar alguno de estos documentos implicaría un retraso en el proyecto debido a que se debería actualizar los documentos realizados hasta el momento.	En caso se concrete este riesgo se procederá a actualizar los documento correspondientes lo más pronto posible.

Riesgo identificado	Impacto en el proyecto	Medidas correctivas para mitigar
Falta de apoyo de la alta dirección.	El apoyo de la alta dirección es básico para el desarrollo de un sistema de gestión, es por ello que sin este apoyo aumentaría significativamente la complejidad del proyecto.	Se firmara una carta de aceptación para certificar el apoyo de la empresa durante el proyecto, adicionalmente se trabajará junto al oficial de seguridad de la información de la entidad pública para coordinar mejor el levantamiento de información en otras áreas.
Rotación de personal dentro de la gerencia de la entidad pública	En caso exista un cambio de personal dentro de la gerencia existe la posibilidad de retraso dentro del proyecto debido a la falta de apoyo de la nueva dirección, especialmente si este cambio se da dentro del comité de seguridad de información.	Antes de empezar a realizar el trabajo de tesis se obtendrá un documento que certifique el apoyo de la empresa al presente proyecto el cual tendrá valor incluso si existe una rotación de personal.

Tabla 1.8.1 - Riesgos identificados del proyecto

2. Capítulo 2: Marco Teórico y Estado del Arte

2.1. Marco Conceptual

A continuación, se presenta la definición de algunos conceptos claves que deben estar claros para la comprensión del tema.

2.1.1. Información

La información es un activo que brinda valor al negocio; por ello, se necesita tener una adecuada protección frente a la constante exposición a distintas amenazas y vulnerabilidades. Esta puede adoptar distintas formas, de ahí surge la importancia de conocerlas para poder protegerla adecuadamente, estas formas son:

- Impresa o escrita en papel
- Almacenada electrónicamente
- Transmitida vía correo o e-mail
- Mostrada en videos
- Hablada en conversaciones
  [NTP ISO/IEC 17799]

2.1.2. Seguridad de Información

Es la protección de la confidencialidad, integridad y disponibilidad de la información; es decir, es asegurarse que esta sea accesible solo a las personas autorizadas, sea exacta sin modificaciones no deseadas y que sea accesible a los usuarios cuando lo requieran [NTP ISO/IEC 17799].

2.1.3. Oficial de Seguridad de Información

El oficial de seguridad de la información, conocido como CISO por sus siglas en inglés (Chief Information Security Officer), es la persona encargada de planificar, presupuestar y verificar el rendimiento de los componentes de la seguridad de la información. Así como de realizar una correcta gestión de riesgo para la toma de decisiones.

Las responsabilidades de cada oficial varían dependiendo de la organización en la que se encuentren, debido a la cultura organizacional que puede existir. [PELTIER; PELTIER; BLACKLEY; 2005]

2.1.4. Política de Seguridad de Información

Las políticas de seguridad de información son aquellas normas que se establecen para guiar a los miembros de la organización a resguardar correctamente la seguridad de la información.

Peltier, en su libro “Information Security Fundamentals”, considera a las políticas de seguridad de información como la piedra angular de una efectiva arquitectura de seguridad de la información, ya que de ella nacen otros documentos importantes tales como directivas, estándares, procedimientos y guías y nos menciona que estas cumplen con 2 roles importantes, un rol interno y otro externo.

- **Rol Interno:** Ya que se menciona a cada uno de los miembros de la organización que se espera que realicen y como se evaluará el trabajo realizado.

- **Rol Externo:** Ya que sirve para mostrarle al mundo como es que se trabaja dentro de la organización, que somos conscientes de la necesidad de proteger nuestra información y la de los clientes y que estamos trabajando para realizarlo.

[PELTIER; PELTIER; BLACKLEY; 2005]

2.1.5. Sistema de Gestión

Un sistema de gestión es una estructura probada para la gestión y mejora continua de políticas, procedimientos y procesos de una organización.
La implementación de un sistema de gestión ayuda a mejorar la efectividad operativa, optimizar costos, lograr mejoras continuas, aumentar la satisfacción de las partes interesadas al negocio y renovar constantemente las estrategias de la organización. [BSI, 2013]

2.1.6. Sistema de Gestión de Seguridad de Información

Conocido como SGSI o ISMS por sus siglas en inglés (Information System Management System) es un sistema de gestión para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información, de esta manera un SGSI lo que busca es poder mantener la confidencialidad, integridad y disponibilidad de la información mientras minimiza los riesgos de seguridad de la información. [NTP ISO/IEC 27001]

2.1.7. Riesgo

Un riesgo es cualquier tipo de evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad. [NTP ISO/IEC 17799]

HALVORSON (2008, 71) explica tres (3) naturalezas del riesgo, estos son los riesgos estratégicos, tácticos y operacionales.
Los riesgos estratégicos son los que pueden estar ligados a la seguridad de la información; sin embargo, se encuentran más orientados a los riesgos de las ganancias y reputación de la organización, ya que se derivan de decisiones estratégicas que han sido tomadas o serán tomadas en la organización.
Los riesgos tácticos son los asociados a los sistemas que vigilan la identificación, control y monitoreo de los riesgos que afectan a la información, son aquellos que afectan indirectamente a la información.
Los riesgos operacionales son los relacionados a aquellos activos que pueden afectar los objetivos de una empresa (tales como presupuestos, cronogramas y tecnologías).

Para poder identificar el potencial daño o perdida debido a un riesgo los dueños de los activos pueden responder estas cuatro preguntas:

- ¿Qué puede suceder? (¿Cuál es la amenaza?)
- ¿Qué tan malo puede ser? (¿Cuál es el impacto?)
- ¿Qué tan seguido puede suceder? (¿Cuál es la frecuencia?)
- ¿Qué tan ciertas son las respuestas de las tres primeras preguntas? (¿Cuál es el grado de confianza?) [OZIER, 2004]

2.1.8. Administrar Riesgos

Es el uso de la información para estimar el impacto de los riesgos e identificar sus causas, de esta manera se pueden tomar medidas anticipadas ante un incidente. [NTP ISO/IEC 17799]

2.1.9. Control

Los controles son medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales. “Una de las clasificaciones más generalizadas es:

- Preventivos: Reducen las vulnerabilidades.
- Detectivos: Descubren amenazas o escenarios previos a ellas permitiendo activar otros controles.
- Correctivos: Contrarrestan el impacto de la ocurrencia de una amenaza.
- Disuasivos: Reducen la probabilidad de ocurrencia de las amenazas.” [TUPIA, 2009]

En el NTP ISO/IEC 17799 también se utiliza el control como un sinónimo de contramedida.

2.1.10. ISO/IEC 27000

Es una norma internacional que busca dar información general sobre los sistemas de gestión de seguridad de información, así como definir algunos términos que son usados por todos los estándares de la familia 27000.

A diferencia de las otras normas de esta familia, esta es de libre distribución y se caracteriza por brindar un listado de las normas mencionadas (véase la figura 2.1.1) junto con una pequeña descripción [ISO/IEC 27000, 2012]:

- **ISO/IEC 27001**: El estándar principal de la familia, brinda los requerimientos para el desarrollo y operación de SGSI incluyendo una lista de controles para el manejo y mitigación de los riesgos asociados a los activos de información. Se puede confirmar la eficacia de la implementación del SGSI mediante una auditoria o certificación

- **ISO/IEC 27002**: Este estándar brinda la guía de implementación de la lista de las mejores prácticas y los más aceptados objetivos de control presentados como anexo en la ISO/IEC 27001, con el objetivo de facilitar la elección de controles para asegurar la seguridad de los activos de información.

- **ISO/IEC 27003**: Este estándar brinda información y una guía práctica para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI según lo establecido por la ISO/IEC 27001.

- **ISO/IEC 27004**: Este estándar provee guías prácticas para el uso de métricas que evalúen la efectividad, objetivos de control y controles usados en un SGSI.

- **ISO/IEC 27005**: Este estándar provee una guía para la gestión de los riesgos de seguridad de información según los requerimientos establecidos por la ISO/IEC 27001.

- **ISO/IEC 27006**: Este estándar se complementa con el ISO/IEC 17021 y brinda los requerimientos necesarios para la acreditación de la certificación de una organización que certifique los SGSI según la ISO/IEC 27001.

- **ISO/IEC 27007**: Provee una guía para conducir una auditoria de un SGSI así como las competencias necesarias de los auditores de sistemas de gestión de seguridad complementando la ISO/IEC 19011

- **ISO/IEC TR 27008**: Es un reporte técnico que brinda una guía para la revisión de la implementación de los controles del SGSI.

- **ISO/IEC 27010**: Provee una guía para gestionar la seguridad de la información en caso la organización intercambie o comparta información importante, ya sea que pertenezca al sector público o privado, que lo haga nacional o internacionalmente, o en el mismo sector u otros sectores del mercado en el que opera.

- **ISO/IEC 27011**: Provee una guía para apoyar la implementación de un SGSI en una empresa de telecomunicaciones.

- **ISO/IEC 27013**: Brinda una guía para la implementación integrada del ISO/IEC 27001 y el ISO/IEC 20000 (gestión de servicios de TI), ya sea implementándolos al mismo tiempo o uno después de otro.

- **ISO/IEC 27014**: Brinda una guía para conocer los principios y procesos del gobierno de la seguridad de la información, que busca que las organizaciones puedan evaluar, dirigir y monitorear la gestión de la seguridad de la información.

- **ISO/IEC TR 27015**: Sirve como complemento a las normas de la familia ISO/IEC 27000 para la implementación, mantenimiento y mejora del SGSI en empresas que provean servicios financieros.

- **ISO/IEC TR 27016**: Es un reporte técnico que brinda una metodología que permite a las organizaciones saber cómo valorar adecuadamente los activos de información identificados, los riesgos potenciales a los activos, apreciar el valor de los controles que protegen a estos activos y determinar el nivel óptimo de recursos que deben ser usados para asegurarlos.

- **ISO/IEC 27799:2008**: Brinda una guía para apoyar la implementación de un SGSI en las empresas de salud con la adaptación del ISO/IEC 27002 según los requerimientos de este sector.

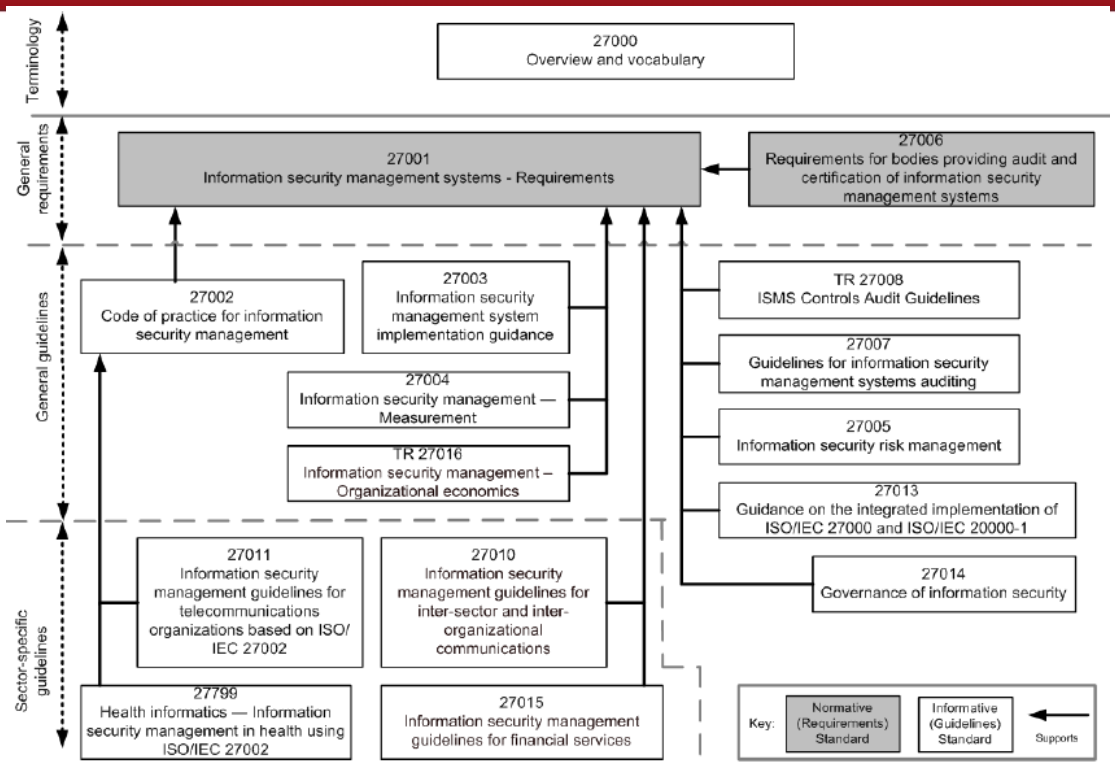

Figura 2.1.1 - Relación de los estándares de la familia del SGSI

Fuente: ISO/IEC 27000 – Tecnologías de información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Información general y vocabulario

2.1.11. COBIT 5

COBIT 5 es un marco integrador que incorpora distintos marcos y estándares para el gobierno de tecnologías de información (IT Governance).

Elaborado por ISACA, contiene las mejores prácticas para el control de los aspectos técnicos y riesgos del negocio permitiendo el desarrollo de políticas para el control de las tecnologías de toda la organización.

En la nueva versión de COBIT podemos observar cinco principios claves para la gestión y gobierno de las TI (véase figura 2.1.2):

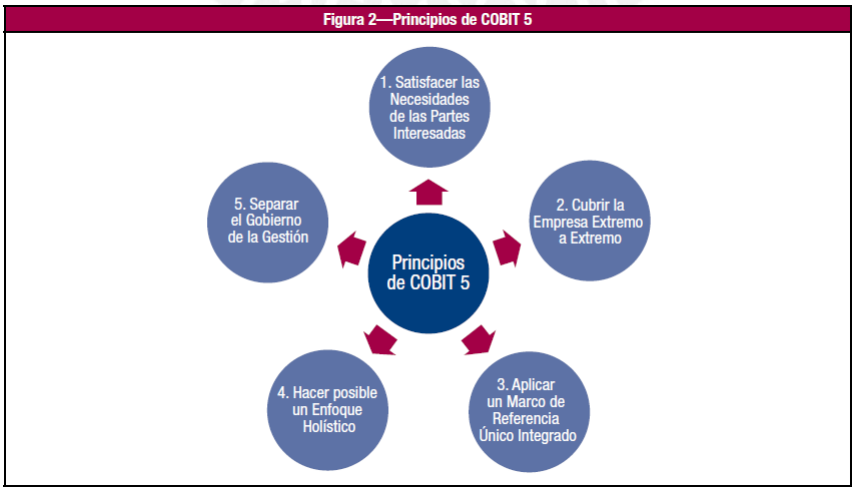

Figura 2.1.2 - Principios de COBIT

Fuente: ISACA - COBIT 5

- **Satisfacer las necesidades de las partes interesadas**
  Al ser un marco referencial, COBIT propone una serie de procesos que pueden ser adaptados según las necesidades propias de cada organización para crear valor en ellas.

- **Cubrir la empresa de extremo a extremo**
  COBIT busca no solo enfocarse en el área de TI de la empresa, sino que busca cubrir todas las funciones y procesos de la organización mediante el uso de catalizadores, los cuales son factores que influyen en el funcionamiento de algo, aplicables a toda la organización

- **Aplicar un marco de referencia integrado y único**
  COBIT se alinea con los distintos estándares, marcos de trabajo y buenas prácticas para ser el marco principal en el gobierno y la gestión de las TI en la organización.

- **Hacer posible un enfoque holístico**
  COBIT define siete categorías de catalizadores para la implementación de un sistema de gobierno y gestión global para las TI, estas categorías son:

  - Principios, Políticas y Marcos de Trabajo
  - Procesos
  - Estructuras Organizativas
  - Cultura, Ética y Comportamiento
  - Información
  - Servicios, Infraestructuras y Aplicaciones
  - Personas, Habilidades y Competencias

- **Separar el gobierno de la gestión**
  COBIT hace una clara distinción entre gobierno y gestión que se puede observar en la figura 2.1.3 [COBIT 5 Framework; 2012]:

  - **Gobierno:** Se encarga de definir los objetivos y planes según los requerimientos de los stakeholders (personas interesadas al proyecto), definen prácticas y actividades para evaluar decisiones estratégicas, dirigir las tecnologías de información y monitorear los resultados.
  - **Gestión:** Son responsables de cumplir los objetivos y las actividades de la organización previamente definidos por el gobierno.

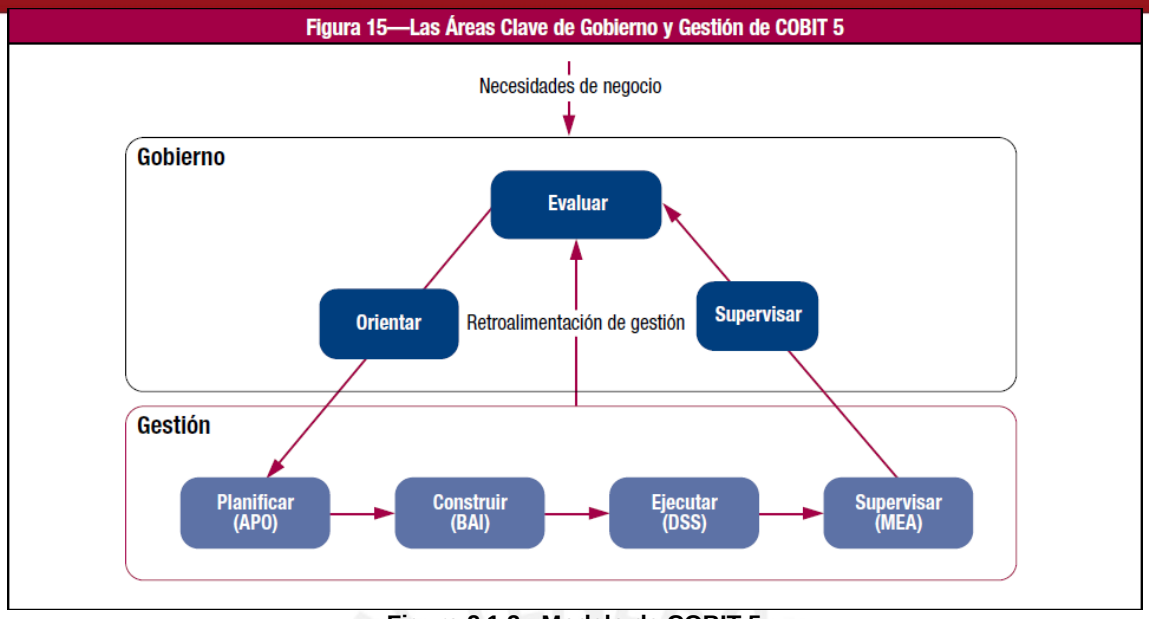

Figura 2.1.3 - Modelo de COBIT 5

Fuente: ISACA - COBIT 5

Adicionalmente se puede observar detalladamente cada uno de los procesos pertenecientes a estas áreas en el grafico 2.1.4

Figura 2.1.4 - Los Procesos habilitadores de COBIT 5.0

Fuente: ISACA - COBIT 5.0

2.1.12. MAGERIT 3.0

El Consejo Superior de Administración Electrónica de España elaboró MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) para gestionar los riesgos de las TIC debido al creciente uso y dependencia de estas para alcanzar los objetivos que cada individuo u organización desea. En esta metodología la gestión de riesgos se divide en 2 subprocesos, estos son:

- **Análisis de Riesgos:**
  Permite determinar lo que posee la organización y que le podría suceder.

- **Tratamiento de Riesgos:**
  Organiza una defensa prudente para sobrevivir a los incidentes y seguir operando en las mejores condiciones, al no poder controlar se maneja un riesgo residual que es asumido por la alta dirección.

De esta manera MAGERIT busca no solo concientizar a los responsables del gobierno de TI de la existencia de riesgos sino que ayuda a descubrir y planificar un tratamiento oportuno para mantener a estos riesgos bajo control.

El método de análisis de riesgos que proporciona MAGERIT consiste en cinco (5) pasos [MAGERIT, 2012]:

1. Determinar los activos relevantes para la organización, sus relaciones entre si y el valor que tienen (según el coste que supondría su degradación)
2. Determinar las amenazas a las que se exponen los activos
3. Determinar las salvaguardas disponibles y que tan eficaces son frente al riesgo
4. Estimar el impacto que tendría una amenaza al dañar un activo
5. Estimar el riesgo

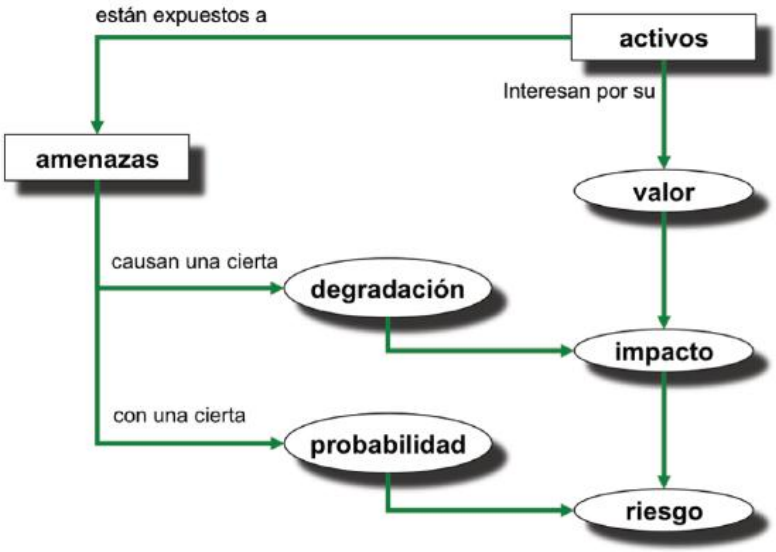

Figura 2.1.5 - Elementos del análisis de riesgos potenciales

Fuente: Consejo Superior de Administración Electrónica de España – MAGERIT – Libro I – Método

2.1.13. OCTAVE

Junto con MAGERIT, OCTAVE es muy reconocido mundialmente, desarrollado por la empresa CERT de la "Carnegie Mellon University" se caracteriza por ser muy resumida en la identificación de activos. Sus siglas significan Operationally Critical Threat, Asset, and Vulnerability Evaluation y es un conjunto de herramientas, técnicas

y métodos para la valoración y planeamiento de la seguridad de la información basada en riesgos.

Actualmente hay tres (3) métodos de OCTAVE:

- El método original
- OCTAVE-S para empresas pequeñas
- OCTAVE-Allegro, un método de valoración de la seguridad de la información más simplificado.

El método original de OCTAVE posee tres (3) fases y ocho (8) procesos los cuales son los siguientes [CERT; 2008]:

1. Generar perfiles de amenazas basados en activos: OCTAVE busca que se defina los perfiles de amenazas según lo que es lo más importante para la organización.

    - Identificar el conocimiento de la alta dirección: Participan los dueños del negocio
    - Identificar el conocimiento de los gerentes del área operativa: Participan los gerentes de mando medio en la organización.
    - Identificar el conocimiento del personal: Es el personal de la organización
    - Crear perfiles de amenazas: Se selecciona que áreas o grupo de personas son las más importantes para el negocio y se identifica a que amenazas son más vulnerable

2. Identificar las vulnerabilidades de la infraestructura: Estas vulnerabilidades pueden ser de diseño, implementación o configuración.

    - Identificar componentes claves: Se revisan los diagramas topológicos de la red para verificar cuales son los componentes claves de la infraestructura
    - Evaluar componentes elegidos: Se corren las herramientas de evaluación de vulnerabilidades escogidas en los componentes elegidos según tres perspectivas, desde afuera de la organización, desde dentro de la organización y desde sistemas incorporados a la organización.

3. Desarrollar una estrategia de seguridad: Una vez se ha identificado los activos, amenazas y vulnerabilidades se continúa con el análisis de riesgo para reducirlo mediante una estrategia acorde a las necesidades de la organización.

    - Conducir análisis de riesgos: Crea unos perfiles de riesgos mediante tres pasos: identificar el impacto de amenazas a los activos críticos, crear criterio de evaluación de riesgos, evaluar el impacto de amenazas a los activos críticos.
    - Desarrollar una estrategia de protección: Se da en dos pasos, el primero es el desarrollo de una estrategia de protección para la organización y planes de mitigación de riesgos a activos críticos y el segundo es la presentación de los planes a la alta dirección para su revisión y decidan qué cambios se harán a la organización basados en estas estrategias.

Las ventajas de usar el método OCTAVE son:

- Es auto dirigido: El personal de TI trabaja junto con pequeños grupos del personal de la empresa que conocen los procesos para encontrar las necesidades de seguridad de la organización.
- Es flexible: Cada método puede ser adaptado a las necesidades de la empresa
- Es evolucionado: OCTAVE ha llevado a las organizaciones a lograr identificar los riesgos que hay en cada proceso del negocio

2.2. Marco regulatorio / legal

Las siguientes resoluciones ministeriales fueron autorizadas por la Presidencia del Consejo de Ministros, las cuales afectan directamente al proyecto de fin de carrera, estas son:

2.2.1. RM-246-2007-PCM

Mediante esta resolución se aprueba el uso obligatorio de la "NTP-ISO/IEC 17799:2007 Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información" en todas las entidades públicas que pertenecen al Sistema Nacional de Informática. Esto significaba el reemplazo de la NTP-ISO/IEC 17799:2004 que en ese tiempo era de uso obligatorio.

2.2.2. RM-197-2011-PCM

Mediante esta resolución se establece como fecha límite para la implementación de la "NTP-ISO/IEC 17799:2007 Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información" el día 31 de diciembre del 2012 para todas aquellas empresas que pertenecen al Sistema Nacional de Informática.

2.2.3. RM-129-2012-PCM

La emisión de esta resolución deja sin efecto la RM-197-2011-PCM, debido a que la norma "NTP-ISO/IEC 17799:2007" que debía ser implementada establece recomendaciones y buenas prácticas de seguridad de información pero no definía una forma exacta de verificar la efectividad y eficiencia de lo que había sido implementado, por lo que la fecha limite dada por esta resolución ya no tenía valor.
Además se define que se debe implementar de manera obligatoria la "NTP ISO/IEC 27001:2008" y da nuevas fechas límites para desarrollar la implementación para todas las empresas públicas (véase figura 1.1.2).
La norma fue emitida el 23 de mayo del 2012, y da 45 días para el inicio de la primera fase por lo que a la primera semana de julio del 2012 debió haberse empezado la misma.

2.3. Estado del arte

Como se mencionó anteriormente, el proyecto busca diseñar un sistema de gestión de seguridad de información para entidades públicas. Debido a ello, se decidió realizar una búsqueda de algunos casos de éxito de implementación de este sistema en entidades públicas tanto a nivel nacional como a nivel regional, buscando resaltar cuales fueron aquellas buenas prácticas utilizadas durante el proyecto que podemos aplicar a nuestra realidad.

2.3.1. Casos de éxito a nivel nacional

Hasta inicios del año 2014, se manejaba poca información sobre el análisis y diseño de un sistema de gestión de seguridad de la información en entidades públicas del Perú. Debemos considerar que, hasta el momento, solo hay ocho empresas que

tienen certificada la ISO 27001, de las cuales, dos pertenecen al sector público, el ONP e INDECOPI, siendo este último la entidad más reciente en conseguirla al haber sido certificada el 17 de abril del año 2013. [INDECOPI; 2013; Noticias]

Revisando algunos casos de éxito de implementación de SGSI en nuestro país, se encontró un proyecto de fin de carrera sobre el diseño de este sistema de gestión aplicado a una compañía de seguros, en el, se presentó algunos factores que son claves para la implementación de un SGSI [AMPUERO; 2011]. En caso alguno de los factores no esté presente durante la implementación del SGSI, podrían actuar de forma negativa para el proceso, aumentando el tiempo del proyecto y en algunos casos deteniéndolo indefinidamente, estos son:

- **Compromiso de la dirección:** Uno de los puntos más críticos en la implementación ya que ellos son los encargados de repartir los roles de seguridad de información, apoyan en la implementación de los controles y son los encargados de administrar los recursos para el proyecto.

- **Consideraciones financieras:** Como parte del proyecto se obtendrá una lista de controles que deberán ser implementados para asegurar los activos críticos de la organización. Debido a esto, es necesario tener un presupuesto para la implementación del SGSI, siendo el oficial de seguridad de información el encargado de calcular el retorno de la inversión de los controles a implementar en la organización.

- **Organización de la seguridad de la información:** Se debe contar con una estrategia que contemple los roles y responsabilidades de cada una de las personas implicadas en el SGSI y que estos sean conscientes de las mismas. Adicionalmente se debe contar con un Comité de Seguridad de Información que informará a gerencia sobre los avances de la implementación del SGSI.

- **Actividades específicas de seguridad:** El autor explica este punto como la implementación del SGSI obedeciendo el marco legal y regulatorio al que está ligado la organización y el uso de algunas normas y estándares que faciliten el seguimiento del SGSI tales como COBIT y la ISO 27002

- **Gestión de riesgos:** Una adecuada gestión de riesgos es muy importante para el desarrollo de un SGSI ya que de ella dependen los controles que serán necesarios para el tratamiento de riesgos.

- **Involucrar a los stakeholders:** Todas las personas involucradas a la organización deben ser conscientes de la implementación del SGSI, los miembros de la organización deben conocer cuáles son sus roles y responsabilidades, la alta dirección debe de apoyar el proyecto para realizarlo exitosamente, los proveedores deberán acoplarse a nuevas exigencias y saber cuál es su rol dentro del SGSI y los clientes conocer que ahora la organización trabaja para mantener su información de una forma más segura.

2.3.2. Casos de éxito y buenas prácticas a nivel internacional

Un segundo trabajo relacionado al estado del arte es una tesis de grado de tres alumnos de la Escuela Superior Politécnica del Litoral de Guayaquil (Ecuador), que trata sobre la implementación de políticas de seguridad basadas en el ISO / IEC 27002 para la municipalidad de Guayaquil.

En esta tesis lo que se busca es brindar una adecuada solución de seguridad de información para la municipalidad de Guayaquil, dentro de la cual se hace el uso de la metodología MAGERIT para el tratamiento de riesgos, argumentando como principal ventaja que las decisiones tomadas por la alta dirección, como resultado del análisis de riesgo, serán fácilmente defendibles y argumentadas.

También se puede observar cuales son las políticas de seguridad propuestas para la municipalidad para los activos físicos, lógicos, equipos de cómputo, respaldo de la información, entre otros.

Adicionalmente se pone a conocimiento cuales son las estrategias de difusión de sus políticas, haciendo especial énfasis en la participación de la alta dirección para facilitar la comunicación de las mismas [BARRAGÁN et al.; 2011].

Finalmente se presenta el desarrollo de un *paper* de la Universidad de Sistan y Bluchestan de Irán (University of Sistan and Bluchestan) que muestra un estudio de los factores de éxito de los sistemas de gestión de seguridad de información en organizaciones municipales de ese país.

El objetivo de esta investigación es identificar la prioridad de los factores clave de éxito en la implementación de sistema de gestión de seguridad de la información en la Organización Municipal de Irán con la opinión de expertos.

Los resultados del estudio mostraron siete factores de éxito ordenados según su prioridad de la siguiente forma:

El primer puesto lo obtuvo el apoyo de la alta dirección debido a que sin él no se podrían implementar los planes organizacionales, el segundo puesto lo ocupan las políticas de seguridad de las organizaciones ya que estas indican que es lo que se puede y se debe realizar.

En el tercer y cuarto puesto se encuentran los programas de capacitación y concientización de la seguridad a los empleados y las responsabilidades laborales respectivamente, donde claramente se puede observar que, después de la alta dirección, es muy importante la participación del personal para poder implementar exitosamente un SGSI en la organización.

En el quinto puesto se tiene el cumplimiento de los estándares internacionales relacionados a seguridad de información, este punto es entendible ya que estos recolectan cuales son las mejores prácticas para poder asegurar eficientemente la información de las distintas empresas.

Un sexto punto indica que los incentivos al personal son útiles en estos casos, lo que lleva al autor a pensar que con buenas políticas de incentivos al personal se podría facilitar la implementación de un SGSI en la organización.

Y por último se expone que la mayoría de organizaciones no considera el apoyo de asesores externos como un factor de éxito. El autor explica que esto se debe, probablemente, a que muchas organizaciones no están dispuestas a adquirir apoyo de profesionales externos debido al gran manejo de información confidencial que puede existir. [Kazemi et al.; 2012]

Con la ayuda de estos cuatro trabajos se puede conocer un poco más como se está trabajando la implementación de los SGSI en las entidades públicas no solo a nivel

local sino a nivel mundial para poder conocer las distintas formas en las que se implementa esta solución del problema.

2.3.3. Marcos de apoyo al SGSI

Debido al marco legal, el problema tiene una única forma de ser resuelta, esto es siguiendo lo indicado por la NTP ISO/IEC 27001:2008. No obstante, se muestra algunos complementos que pueden utilizarse para apoyar la implementación del SGSI.

Como parte de las buenas practicas propuestas en el área de TI, se recomienda el uso de COBIT 5, un marco integrador elaborado por ISACA que contiene algunas buenas prácticas para el control de riesgos del negocio y orienta a la gestión y gobierno de TI [COBIT 5], esto debido a su amplia cobertura y porque está basado en muchas practicas existentes. La ventaja de implementarlo en la organización es que ayuda a los ejecutivos a comprender y gestionar las inversiones de TI durante su ciclo de vida [ITGI, OGC; 2008], de esta manera, las empresas pueden utilizar las TI para tener ventajas comerciales frente a sus competidores. Una ventaja adicional es que, al ser un marco integrador, permite el uso de otras normas y marcos acoplándolos fácilmente.

No obstante, COBIT solo se focaliza en lo que necesita hacer la empresa pero no en cómo debe hacerlo por lo que recibe el apoyo de otros marcos y normas, tal es el caso de ITIL, que actualmente se encuentra en su versión 3.0, se caracteriza por respaldar los procesos de negocio de la organización así como por gestionar los servicios de TI

Si bien implementar COBIT e ITIL sería una gran ventaja para la organización, esto escapa del alcance del presente proyecto ya que también se encarga de la gestión del gobierno de TI de la organización; sin embargo, se proporcionará un enlace de la publicación de ITGI y OGC donde se mapean tanto los procesos y objetivos de control de COBIT a secciones específicas de ITIL e ISO/IEC 27002 como de manera inversa, mostrando como las secciones de ITIL y los objetivos de control del ISO/IEC 27002 mapean a los objetivos de control de COBIT [ITGI, OGC; 2008]. Si bien la versión de COBIT que es mapeada es la 4.1, será de gran ayuda para tener como base en caso se deseen implementar estos marcos en algún proyecto, previa actualización de COBIT.

2.3.4. Conclusiones sobre el estado del arte

La implementación de un SGSI trae grandes ventajas a las organizaciones, por ello, es comprensible el deseo del gobierno peruano de su realización en las distintas empresas públicas; no obstante, para muchas personas puede aún no estar claro cuáles son los pasos a seguir o los requisitos necesarios para poder implementarlo, como clara evidencia de ello es que, a mayo del 2013, pocas entidades públicas habían validado con la ONGEI el alcance de sus SGSI.

Como resultado de todos los trabajos relacionados se puede observar la clara necesidad de una adecuada evaluación de los riesgos según las necesidades de la organización, independientemente de la metodología usada, esto debido a que cada empresa se rige ante un marco legal distinto dependiendo del sector y del país donde se desempeñe.

También cabe recalcar la importancia del constante apoyo de la alta dirección ya que no es una responsabilidad únicamente del área de TI; debe fluir desde arriba hasta todos los procesos de negocio, adicionalmente, la alta dirección debe mostrar un claro

interés por el desarrollo del proyecto participando activamente del mismo, ya sea apoyando en la difusión de las políticas o velando por la mejora continua del SGSI.

Asimismo, se debe tener en cuenta los resultados del estudio realizado en Irán, que probablemente no sean muy distintos de la realidad peruana, ya que se observa la necesidad del compromiso de la alta dirección tanto en los resultados de este estudio como en los principales problemas detectados por el ingeniero Horna.

Basados en este último punto es muy necesario, que cada uno de los empleados de la organización conozca cuál es su rol dentro de este sistema de gestión para que se sientan comprometidos con el proyecto y puedan aportar positivamente a su implementación con la ayuda de una previa capacitación y concientización de la seguridad en su puesto laboral.
Por último, se puede concluir que la norma busca organizar a las empresas para que, con este orden adquirido, se pueda gestionar mejor la seguridad de los activos de información. Es por ello que este proyecto busca dos cosas:

- Brindar una base para la implementación de un SGSI, de esta manera cualquier empresa pública podría adecuar y complementar este trabajo según las necesidades propias de la empresa.

- Ayudar a una empresa pública con la primera etapa del ciclo de Deming (Plan – Planear) en la implementación del SGSI, enfocado a los procesos críticos de esta empresa, desde el modelamiento de los procesos que pertenezcan al alcance del proyecto, hasta el análisis de riesgo de los activos y la declaración de aplicabilidad.

De esta forma no solo se busca apoyar a una organización para gestionar la seguridad de su información, también busca brindar una guía para el análisis y diseño de un SGSI en todas las empresas públicas que se encuentran en la Fase I o II de las fases de implementación incremental de la NTP ISO/IEC 27001 (véase figura 1.1.1).

3. Capítulo 3: Documentación Necesaria para el Diseño de un SGSI

3.1. Business Case

Como se discutió dentro del estado del arte, obtener el total apoyo de la alta dirección es crucial para el desarrollo del proyecto. Adicionalmente, la NTP ISO/IEC 27001 indica que se debe buscar obtener este compromiso dentro de la fase inicial del proceso de implementación. Ante esta situación, se desarrolló un documento que permita evidenciar ante la gerencia cual es la situación actual de la organización, la problemática que enfrentan y que opciones se posee para atender estas nuevas necesidades.

Dentro del documento, se presentó cinco (5) opciones para solucionar la problemática, siendo la más recomendable la implementación de la norma NTP ISO/IEC 27001:2008 con el apoyo de una empresa consultora especialista en el tema, decisión basada en tres criterios principales:

- Cumplimiento del marco legal
- Costo Efectividad
- Recomendación del personal de la ONGEI

Adicionalmente, se recomendó enfocar el proyecto de implementación de la norma en dos etapas, una etapa de planificación y diseño y otra etapa de despliegue, esto ya que es más fácil calcular el costo de la etapa de despliegue, una vez se culmine con la primera etapa y debido al poco tiempo que queda para culminar con la implementación de la norma.

Este documento puede ser visualizado en su totalidad dentro de los anexos del presente proyecto como “Anexo 4 – Modelo de Caso de Negocio”

3.2. Alcance Formal del Proyecto

Según lo trabajado con la institución, el alcance cubrirá todos los procesos relacionados a la atención de los clientes empresariales a nivel local (Lima), este alcance cubre los siguientes procesos del área postal realizados en la sede central de SERPOST:

- Admisión
- Habilitado
- Clasificación
- Control de Cargos
- Digitalización
- Facturación

Y al proceso de Distribución realizado en la Administración Postal de Miraflores.

Este documento puede ser consultado como “Anexo 2 – Alcance Formal del SGSI”, adjunto al presente trabajo. Sin embargo, el presente proyecto de fin de carrera presenta un alcance distinto al definido por la organización ya que, basándose en el alcance definido por la organización, se delimitó a los siguientes procesos:

- Admisión
- Habilitado
- Clasificación
- Control de Cargos
- Digitalización

Los cuales se desarrollan íntegramente en la sede central de SERPOST o CCPL, ubicada en el distrito de Los Olivos.

3.3. Política de Seguridad de Información

La NTP ISO/IEC 27001:2008, exige en el inciso b, numeral 4.2.1, la definición de una política de seguridad de información que brinde un marco referencial para establecer los objetivos y un sentido de dirección para la seguridad de la información. [NTP ISO/IEC 27001:2008], debido a ello, se desarrollaron diversas entrevistas con cada uno de los miembros del comité de seguridad de la información para conocer sus expectativas, sus necesidades y sus preocupaciones con respecto a este sistema de gestión.

La política de seguridad de la información debe ser parte de un documento general de la política empresarial [NTP ISO/IEC 17799:2007], debido a ello, debe ser aprobada por el comité de seguridad de la información y de conocimiento de la plana gerencial, buscando en todo momento su aceptación y compromiso para que pueda ser distribuida a toda la empresa a través de ellos.

Es necesario aclarar que este tipo de documentos deben ser revisados y actualizados regularmente para evitar que queden en el olvido o reflejen una realidad distinta a la que la organización está atravesando, es por ello que es necesario no solo definir la política de seguridad, también es necesario definir los roles y responsabilidades de las personas con respecto al sistema de gestión, la frecuencia con la que se revisará este documento y las sanciones que se aplicarán en caso no se cumpla con lo indicando.

Como resultado de las entrevistas realizadas se obtuvo dos documentos, uno de la política de seguridad de información, en la cual se definió los roles y responsabilidades, frecuencia de revisión y la política en sí, y otro sobre los objetivos del SGSI.

Ambos documentos pueden ser consultados como “Anexo 1 – Política de Seguridad” y “Anexo 3 – Objetivos del SGSI”, respectivamente, adjuntos al presente trabajo.

4. Capítulo 4: Identificación y Valoración de los Activos de Información

4.1. Mapa de procesos relacionados al sistema de gestión

En el presente capítulo se mostrará cómo se realizan aquellos procesos que están involucrados en el alcance del SGSI, para ello, se realizaron varias entrevistas con los dueños de los procesos para recolectar la información necesaria de cómo es que realizan su trabajo en el área.

Para realizar el modelado de procesos, se decidió utilizar la notación BPMN 2.0 (Business Process Modeling Notation) a fin de facilitar la labor de análisis y evaluación de riesgos una vez identificados los activos involucrados al sistema, esto debido a que nos permite graficar una serie de eventos, definir los tipos de tareas con las que se está trabajando y asociar los activos identificados dentro del proceso a una tarea específica. Sin embargo, debido a que el personal no conocía esta notación y a la empresa le interesaba tener los procesos mapeados, no solo se trabajó con BPMN, sino que también se utilizaron diagramas de flujo.

4.1.1. Proceso de Recepción

El primer proceso relacionado a la atención de clientes empresariales, se divide en dos subprocesos, el primero es el proceso de admisión, mientras que el segundo proceso es de habilitado. Ambos subprocesos son realizados en el área de Extra postales.

a) Proceso de Admisión

Presentado como Anexo 11, el objetivo de este primer subproceso es el de recibir cada uno de los envíos de los clientes empresariales para la generación de la guía de admisión y pase al proceso de habilitados

Participan de este proceso los postrenes, personas encargadas de realizar entregas de cargos y recojo de envíos de los clientes, los operadores postales quienes realizan el proceso de admisión como tal.

El proceso empieza una vez el área de Extra postales de la empresa recibe una copia del contrato que se ha realizado con un cliente indicando la cantidad de envíos que va a recibir, si debe recogerlos de algún local o si los recibirá en la misma sede central, así como otros datos tales como la fecha máxima para la entrega, tipos de entrega, servicios adicionales requeridos y penalizaciones. Una vez recibidos, se encarga de generar una guía de admisión y derivarla al proceso de habilitado.

b) Proceso de Habilitado

Presentado como Anexo 12, el objetivo de este sub proceso es el preparar cada uno de los envíos solicitados por los clientes, según las indicaciones dadas en el contrato, para que puedan ser enviadas a los destinatarios finales.

Participan de este proceso los operadores postales, encargados de imprimir los cargos necesarios, adjuntarlos a los envíos, ingresar los datos al sistema y preparar los envíos según lo solicitado por el cliente.

El proceso empieza una vez los operadores postales generan la guía de admisión, de haber sido solicitado por los clientes, se deberá etiquetar los cargos de los clientes en los envíos, así como, de habilitar los envíos, es decir, de desglosarlos, doblarlos, ensobrarlos, encartarlos, engomarlos, embolsarlos, etiquetarlos o engramparlos con algún objeto adicional. Por último se elabora una guía de salida y se envía al área de clasificación para que pueda enviarlos a los destinatarios finales.

Adicionalmente, una vez los envíos fueron entregados, este proceso incluye el tratamiento de la guía de salida, el cierre de la guía de admisión y la búsqueda de la conformidad del cliente, actividades a cargo del supervisor del área.

4.1.2. Proceso de Clasificación

a) Proceso de Clasificación

Presentado como Anexo 13, el objetivo de este subproceso es el de separar cada envío según sectores existentes dentro de las administraciones postales para su envío.

Participan de este proceso los clasificadores encargados de la sectorización.

El proceso inicia una vez el área de extra postales hace entrega de envíos con la guía de salida, un operador postal es el encargado de abrir cada saca y verificar si la cantidad entregada es la misma que la indicada en dicha guía, una vez verificado, se hace entrega de los envíos a los clasificadores, para que se encarguen de dividirlos según administración postal destino y el sector correspondiente. Una vez realizada la separación se confeccionan las sacas para su envío a cada administración postal

b) Sub Proceso de Pre clasificación

Presentado como Anexo 14, el objetivo de este subproceso es el de separar cada uno de los envíos recibidos del área de extra postales por centro de distribución y guía de salida, a fin de facilitar el proceso de clasificación.

Participan de este proceso los operadores postales, encargados de abrir las sacas enviadas por extra postales y de entregar los envíos a los clasificadores para que se encarguen de dividir cada envío por administración postal.

El sub proceso inicia una vez se dan los envíos a los clasificadores. Ellos se encargan de dividirlos según administración postal destino en un proceso que puede ser manual o con la ayuda de un sistema de información, dependiendo de la solicitud del cliente. Una vez realizada la separación se envía al proceso de clasificación final.

4.1.3. Proceso de Control de Cargos

a) Proceso de Control de Cargos

Presentado como Anexo 15, el objetivo de este proceso es el de controlar la cantidad de envíos que fueron entregados correctamente y la cantidad de envíos que se devolvieron por no tener problemas al momento de ser entregados.

Participan de este proceso tanto el operador postal que es el encargado de realizar el conteo e ingreso al sistema de la cantidad de envíos entregados y devueltos y los postrenes, encargados de entregar documentos a los clientes para que reciban su aprobación.

Este proceso se encarga de recibir los cargos y despachos de los clientes, verificar que los datos sean correctos y, de requerirlo, mandar a digitalización los cargos y rezagos o solo digitarlos en el sistema, una vez finalizado este proceso se genera un reporte de devolución, el cual será enviado al cliente junto con los rezagos a través del postren.

b) Proceso de Emisión de Reporte de Facturación

Presentado como Anexo 16, el objetivo de este proceso es el de emitir los reportes de facturación, según los servicios brindados a los clientes, para que el área de facturación pueda realizar los cobros respectivos.

Participan de este proceso tanto el operador postal que es el encargado de emitir los reportes de cargos devueltos y almacenarlos una vez tengan el visto bueno de los clientes y el supervisor, encargado de generar los reportes de facturación para los clientes y el área de facturación.

Este proceso inicia una vez el postrén regrese con el reporte de devolución aprobado por el cliente, esta guía deberá ser archivada dentro del área y, en caso lo solicite el cliente, se generará un reporte de facturación para el cliente, el cual deberá ser enviado al mismo para que pueda dar su visto bueno y sea enviado al área de facturación, en caso el cliente no desee este reporte, solo será generado para el área de facturación.

4.1.4. Proceso de Distribución

a) Proceso de Digitalización

Presentado como Anexo 17, el presente proceso tiene como objetivo digitalizar cada uno de los envíos y rezagos para que puedan ser mostrados en la extranet de la organización y sean almacenados en algún dispositivo digital.

Participan de este proceso, los digitalizadores, encargados de pasar la información de formato físico a digital

El proceso inicia una vez que el área de control de cargos hacen entrega de los cargos y rezagos que se deben de digitalizar, dentro del área se encargan de escanear cada uno de esto documentos y de enlazarlos a las guías de admisión con la ayuda de lectoras de códigos de barras.

Una vez digitalizados se suben a la base de datos y a un servidor web desde el cual podrán ser visualizados por los clientes que así lo hayan requerido.

b) Proceso de Elaboración de Reportes y CD’s

Presentado como Anexo 18, el presente proceso tiene como objetivo enviar, a cada uno de los clientes, las imágenes digitalizadas en un dispositivo de almacenamiento en caso lo soliciten, adicionalmente se encarga de emitir los reportes de facturación para los clientes y el área de facturación por los servicios realizados por cada cliente.

Participan de este proceso la supervisora, encargada de la realización de CD con las imágenes digitalizadas y las bases de datos cuando el cliente lo solicita.

El proceso inicia una vez el cliente solicite un servicio de respaldo de información en CD, haciéndoles entrega de las imágenes digitalizadas, así como de la base de datos de los envíos actualizada. Adicionalmente, la encargada del área se encarga de la generación de reportes por los servicios prestados a cada uno de los clientes atendidos.

4.2. Identificación de los activos de información

Una vez mapeado cada uno de los procesos que forman parte del alcance del proyecto, se debe realizar una serie de entrevistas para identificar cada uno de los activos de información que están involucrados en los procesos, luego se procederá a valorarlos y asegurar cada uno de los activos más importantes para la organización.

Para la identificación de estos activos se utilizó el mapa de procesos durante cada una de las entrevistas, ya que permitió asociar los activos con una actividad del proceso.

El objetivo de esta parte del proyecto es obtener un inventario de los activos de información involucrados en el alcance del SGSI, para ello se desarrolló una metodología de valoración de activos, basada en lo propuesto por la ISO/IEC 27005:2008, en la cual se detalla cual es el procedimiento para la identificación de los mismos, esta metodología puede ser consultada en el “Anexo 5 – Metodología de Valoración de Activos” del documento.

Para la realización del inventario de activos se tomó en cuenta los siguientes datos:

- Id Activo: Un código que pueda identificar a los activos de información.
- Proceso: El proceso en el que se encuentra el activo de información
- Actividad: Cual es la actividad específica, dentro del proceso, en el cual se encuentra el activo de información.
- Nombre: El nombre del activo
- Descripción: Una descripción breve de cada uno de los activos de información.
- Tipo de Activo: Si es primario o secundario, según lo definido en la metodología.
- Proveedor de la Entrada: De qué área o actor proviene el activo
- Receptor de la Salida: A qué área o actor se envía el activo
- Propietario del Activo: Quien es el dueño del activo de información
- Ubicación: Cual es la ubicación física o lógica del activo de información
- Formato: En que formato se encuentra el activo, si es papel, electrónico, verbal u de otro tipo.
- Clasificación Actual del Activo de Información: La rotulación actual del activo (público, interno, privado, restringido).

4.3. Valoración de los activos de información

Una vez identificados cada uno de los activos involucrados en el alcance del SGSI, se debe valorar cada uno de ellos para seleccionar aquellos que pasarán al análisis de riesgo, para ello, se realizaron entrevistas con los dueños de los procesos para responder a la siguiente pregunta ¿De qué manera la pérdida del activo impacta a la confidencialidad/integridad/disponibilidad de la información?

Durante las entrevistas, se utilizó la siguiente tabla de valoración:

Valor	Dimensión		
	Confidencialidad	***Integridad***	***Disponibilidad***
1	No existe ningún riesgo legal, reputacional, operacional, ni financiero si la información es publicada o es de conocimiento del público en general	Debe ser correcto y completo al menos el 25% de las veces. No existe ningún riesgo legal, reputacional, operacional, ni financiero en la toma de decisiones	Debe estar disponible al menos el 25% de las veces que se necesita. No existe ningún riesgo legal, reputacional, operacional, ni financiero si la información no está disponible o ha sido destruida
2	La divulgación no es perjudicial para los intereses legal, reputacional, operacional, ni financiero pero debiera ser sólo de conocimiento de los colaboradores.	Debe ser correcto y completo al menos el 50% de las veces. Podría ocasionar daños leves para los intereses legales, reputacionales, operacionales y financieros de la organización si se toman decisiones sobre ésta	Debe estar disponible al menos el 50% de las veces que se necesita. Podría ocasionar daños leves para los intereses legales, reputacionales, operacionales y financieros de la organización si no estuviera disponible o hubiera sido destruida
3	Información personal, financiera o de alguna sensibilidad. Su divulgación podría ser perjudicial para los intereses de la organización.	Debe ser correcto y completo al menos el 75% del as veces. Podría ser perjudicial para los intereses legales, reputacionales, operacionales y financieros de la organización si se toman decisiones sobre ésta	Debe estar disponible al menos el 75% de las veces que se necesita. Podría ser perjudicial para los intereses legales, reputacionales, operacionales y financieros de la organización si no estuviera disponible o hubiera sido destruida
4	Información altamente sensible. Su divulgación podría causar daños catastróficos, reputacionales e imagen, pérdidas financieras significativas.	Debe ser correcto y completo el 100% de las veces. Podría causar daños catastróficos, reputacionales e imagen, pérdidas financieras significativas de no ser exacta.	Debe estar disponible el 100% de las veces que se necesita. Podría causar daños catastróficos, reputacionales e imagen, pérdidas financieras significativas de no estar disponible.

Una vez valorados todos los activos previamente identificados se escogerán aquellos cuyo valor promedio de confidencialidad, integridad y disponibilidad sea mayor a 2

En el “Anexo 7 – Inventario y Valoración de Activos” se puede encontrar el inventariado de los activos relacionados al alcance del SGSI y valorados por los usuarios.

5. Capítulo 5: Identificación y Evaluación de Riesgos

El objetivo del presente capítulo es la elaboración de la Matriz de Riesgos de la organización, para ello se definió una metodología de evaluación de riesgos, en la cual se describía cual era el apetito de riesgo de la organización, el procedimiento para la identificación de riesgos y el criterio para la evaluación de los mismos.

Para el desarrollo de esta metodología se utilizó la norma ISO/IEC 27005:2008, la cual brinda una guía sobre la gestión de riesgos en la seguridad de la información, y se adaptó según las necesidades de la organización, esta metodología puede encontrarse en el "Anexo 6 – Metodología de Análisis de Riesgos". Los pasos involucrados dentro de ella son:

5.1. Identificación del Riesgo

El primer paso dentro de la metodología es la identificación de las amenazas y vulnerabilidades, para ello, se deberá escoger aquellos activos de información que fueron considerados los más importante en la identificación y valoración de activos y se evaluará a que amenazas y vulnerabilidades se encuentran expuestas.

Para realizar este trabajo de identificación de riesgos, es necesario definir lo que es una amenaza, vulnerabilidad y riesgo. En la metodología de evaluación se define a las amenazas como aquellos eventos o actividades que pueden dañar o afectar a los activos de información.

Las vulnerabilidades no pueden dañar a los activos por si solos, ya que son características propias de estos; sin embargo, deben ser identificadas debido a que son fuentes potenciales de riesgos en caso logren ser explotadas por alguna amenaza.

Por último, los riesgos se definieron como aquella probabilidad de que una amenaza explote alguna vulnerabilidad haciéndole perder alguna propiedad relacionada a la seguridad de la información (confidencialidad, disponibilidad, integridad, auditabilidad, etc.), de ahí la necesidad de identificar las amenazas y vulnerabilidades previamente.

Para ello se realizaron visitas al área donde se llevan a cabo los procesos pertenecientes al alcance del SGSI y se utilizó una lista de ejemplos de vulnerabilidades y amenazas proporcionadas por el Anexo D de la ISO/IEC 27005:2008, la cual se puede visualizar en los anexos del proyecto como "Anexo 8 - Lista de Ejemplos de Vulnerabilidades y Amenazas"

Una vez identificados los riesgos se llevó a cabo una entrevista con cada uno de los dueños de los procesos para que corroboren si los riesgos son reales y si es que ellos han identificado algún riesgo que no haya sido previamente mapeado para agregarlo a la matriz.

5.2. Evaluación del valor de riesgo.

Una vez identificados los riesgos, se procederá a evaluar, junto con los dueños de los procesos, cuáles son las probabilidades de ocurrencia y los impactos que traerían a la organización en caso se materialicen estos riesgos, para ello podrán usar las escalas desde "Muy Baja" hasta "Muy Alta" para las probabilidades y una escala de "Insignificante" hasta "Catastrófica" para el impacto.

A continuación se presentan las tablas con las escalas de valoración de probabilidades e impactos y el criterio utilizado

Lista de Probabilidades			
Nivel	**Descripción**	**Escala de porcentaje**	**Probabilidad**
5	Muy Alta	Más de 80%	Ocurrirá en la mayoría de las circunstancias; todos los días o varias veces al mes.
4	Alta	60% - 80%	Probablemente ocurrirá en la mayoría de las circunstancias; al menos una vez al mes.
3	Moderada	40% - 60%	Puede ocurrir en algún momento; al menos una vez al año.
2	Baja	20% - 40%	Podría ocurrir en algún momento; al menos una vez cada dos años.
1	Muy Baja	Menos de 20%	Puede ocurrir en circunstancias excepcionales; como dos veces cada cinco años.

Lista de Niveles de Impacto		
Nivel	**Descriptivo**	**Explicación**
8	Catastrófica	Pérdida o daño catastrófico a la reputación de la organización; pérdidas financieras importantes, cobertura a nivel nacional y de forma prolongada; intervención regulatoria con sanciones por faltas muy graves; pérdida de clientes a gran escala; involucramiento directo de la alta gerencia o directorio.
6	Mayor	Daño sobre la empresa es mayor, riesgo inusual o inaceptable en el sector; cobertura a nivel nacional; investigación del regulador y sanciones por falta grave; involucramiento de la alta gerencia, gastos operativos de consideración; pérdidas financieras mayores.
4	Moderado	El impacto sobre la compañía es directo y medio, se podría incurrir en gastos operativos controlados, existen sanciones por falta leve, se expone la imagen de la organización con un impacto medio.
2	Menor	Riesgo aceptable en el sector; no hay daño a la reputación, no hay sanciones legales, pero si observaciones por parte de los reguladores, el impacto operacional o financiero es mínimo.
1	Insignificante	No hay impacto directo sobre la organización, no hay daño a la reputación, no existen sanciones legales ni impacto financiero u operacional; no es percibido por los clientes pero si por los colaboradores.

Una vez que se haya valorizado la probabilidad e impacto de cada uno de los riesgos detectados, se realizará una multiplicación entre estos valores para conocer el valor del riesgo, dependiendo del valor hallado se conocerá el nivel del riesgo con la ayuda de la siguiente matriz de calor:

IMPACTO						
	8	8	16	24	32	40
	6	6	12	18	24	30
	4	4	8	12	16	20
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	**2**	**3**	**4**	**5**
		PROBABILIDAD				

Junto con el comité de seguridad de la información, se definió tres niveles de riesgo graficados en la matriz anterior, estas son:

- ***Riesgos Bajos***: Aquellos riesgos cuyo valor oscila entre 1 y 8. Riesgos inferiores, deben ser tratados con los procedimientos de rutina ya definidos en la organización. Es hasta este punto en el cual se define el Apetito de Riesgo de SERPOST, es decir, aquellos riesgos que no se encuentren en esta zona deberán ser tratados con ayuda de controles para minimizar su valor.
- ***Riesgos Altos***: Aquellos riesgos cuyo valor oscila entre 9 y 18. Riesgos que deben ser tratados con procedimientos especiales con la ayuda de la implementación de algunos controles de seguridad, la Alta Dirección debe ser consciente de la existencia y tratamiento de estos riesgos.
- ***Riesgos Graves***: Aquellos riesgos cuyo valor oscila entre 20 y 40. Riesgos que deben ser tratados de manera inmediata y con alta prioridad debido a lo que podría suceder si se materializa el riesgo, la Alta Dirección debe ser consciente de la existencia y tratamiento de estos riesgos.

5.3. Apetito de Riesgo de la Organización

Como se señaló previamente, el apetito de riesgo de la organización involucra aquellos riesgos cuya multiplicación de impacto y probabilidad oscila entre 1 y 8, es decir, solo los riesgos bajos, debido a ello, se recomendó monitorearlos para evitar que su probabilidad o impacto crezca en el tiempo.

Cualquier riesgo que exceda estos valores, deberá ser tratado de manera inmediata para reducir su valor a un rango aceptable por la organización según lo indicado por la metodología de evaluación de riesgos.

5.4. Tratamiento del Riesgo

Una vez identificados aquellos riesgos que amenazan a la organización, se deberá evaluar con la ayuda de la NTP ISO/IEC 17799:2007, cuales son los controles que se deben implementar para el tratamiento de riesgos.

Según la naturaleza del riesgo, las acciones que se pueden realizar para tratarlo pueden ser: “Mitigar” el riesgo, “Transferir” el riesgo, “Eliminar” el riesgo o “Aceptar” el riesgo, la definición de cada una de estas acciones se encuentra a continuación:

Tratamiento	Descripción
Mitigar	Reducir los riesgos mediante la implementación de controles que reduzcan el riesgo a un nivel aceptable. Estos controles deberán presentar una documentación adecuada para su implementación y puesta en marcha.
Aceptar	En este escenario se decide no tratar el riesgo debido a no haber identificado controles adecuados para el tratamiento de los riesgos o haber identificado que el costo de implementar algún control es mayor que los beneficios que se obtendrán. Toda aceptación del riesgo debe ser documentada y firmada por el Comité de Seguridad de la Información indicando los criterios de esta decisión. Por último, deberán ser constantemente monitoreados en caso evolucionen y se conviertan en riesgos más graves.
Transferencia	Alternativa más económica en caso sea muy costoso o difícil reducir o controlar un riesgo. Sin embargo, al transferir un riesgo no se transfiere las responsabilidades por lo que deberán ser constantemente monitoreadas para asegurarnos de su correcto tratamiento.
Eliminar	Una de las alternativas más difíciles de implementar y más costosas ya que puede implicar la eliminación de un activo, proceso o del área del negocio que es fuente de riesgo. Este plan de tratamiento debe estar debidamente justificado y documentado en caso se decida implementar. Adicionalmente se debe realizar un nuevo Análisis de Riesgo teniendo en cuenta el cambio realizado en la organización.

De igual forma, los controles pueden ser clasificados de la siguiente forma:

Tipo de Control	Descripción
Preventivo	Como su nombre lo indica, son controles que buscan prevenir la materialización de un riesgo, mediante un adecuado control de las vulnerabilidades de un activo.
Detectivo	Este tipo de controles busca ***descubrir*** nuevos riesgos antes que se materialicen, de tal forma, que puedan ser controlados con anticipación
Correctivo	Son controles que se encargan de corregir alguna incidencia minimizando el ***impacto*** del daño o pérdida originada por el riesgo.
Disuasivo	Son controles que buscan reducir la ***probabilidad*** de ocurrencia de algún riesgo.

5.5. Matriz de Riesgo

Por último, una vez realizado todo el análisis descrito anteriormente, el oficial de seguridad de la información deberá asegurarse de ingresar todos esos datos en la matriz de riesgo de la organización para presentar el resultado al comité, el cual decidirá si hay algún riesgo que aceptar o si dará tratamiento a todos los riesgos.

Entre las varias columnas que posee la matriz de riesgo se tiene:

- Id Riesgo: Identificador único del riesgo.
- Proceso: Nombre del proceso en el cual se detectó el riesgo.
- Nombre del Activo: Nombre del activo en el que se detectó el riesgo.
- Valoración del Activo: Los puntajes de confidencialidad, integridad y disponibilidad que le fueron otorgados al activo de información.
- Amenaza: La descripción de la amenaza que acecha al activo de información.
- Vulnerabilidad: La descripción de la vulnerabilidad del activo de información.
- Riesgo: Descripción del escenario en caso la amenaza explote la vulnerabilidad.
- Probabilidad: Probabilidad que el riesgo se materialice.
- Impacto: El nivel de impacto en caso el riesgo se materialice.
- Nivel de Riesgo: Multiplicación de la probabilidad e impacto del riesgo.
- Valor del Riesgo: El nombre de la zona en la que se encuentra el riesgo. (Bajo, Altos o Graves)
- Tipo de Tratamiento: Se colocará el tipo de tratamiento que se le dará a los riesgos identificados (Mitigar, Aceptar, Transferir o Eliminar)
- Control Alineado a la NTP ISO/IEC 17999: Control o controles sugeridos por la NTP para el tratamiento de un riesgo identificado.
- Control Especifico: Control o controles basados en los sugeridos por la NTP y alineados a las necesidades de la empresa
- Tipo de Control: Se colocará el tipo de control que se le ha elegido (Preventivo, Detectivo, Correctivo o Disuasivo)
- Responsable: Persona responsable del tratamiento del riesgo.

La matriz de riesgo correspondiente al alcance del SGSI se podrá visualizar en los anexos del documento como “Anexo 9 – Matriz de Riesgos”

6. Capítulo 6: Declaración de Aplicabilidad

La norma NTP ISO/IEC 27001:2008, exige como parte del establecimiento del SGSI, en el punto 4.2.1, la preparación de la declaración de aplicabilidad incluyendo cuales son los objetivos de control y los controles seleccionados justificando su elección.

Estos controles son sacados del anexo A de la NTP ISO/IEC 27001:2008 y de la NTP ISO/IEC 17799:2007, las cuales brindan una serie de controles y recomendaciones para el tratamiento de los riesgos en una organización.

En este documento se analizará cada uno de los controles propuestos por estas normas y se indicará si son aplicables a la realidad de la empresa o si no lo son, justificando en ambos casos el porqué de esta decisión.

Este documento puede ser revisado como anexo del presente proyecto con nombre "Anexo 10 – Declaración de la Aplicabilidad" y muestra la siguiente información:

- N° de Control: El identificador de cada uno de los controles propuestos por la norma
- Control: El nombre del control, se hace referencia a un tema específico al que un riesgo puede estar asociado.
- Objetivo de Control: Es la descripción del control, en él se indica exactamente a que se refiere cada uno de los controles de la norma.
- Aplicable a la organización: Se indica si el control en mención es aplicable a la organización o si no lo es.
- Justificación: La justificación de la aplicabilidad o no aplicabilidad del control en mención.

7. Capítulo 7: Conclusiones y Recomendaciones

A continuación, se presentará cuales fueron aquellas conclusiones y recomendaciones resultantes de haber realizado el diseño de un SGSI en una entidad pública perteneciente al sector postal.

7.1. Observaciones

- Como bien se indicó dentro del presente proyecto, el apoyo de la alta gerencia es vital para el éxito de este tipo de proyectos, uno de los principales problemas que se encontró durante el desarrollo del mismo fue la poca preocupación para la implementación de este sistema de gestión en la organización, no fue sino hasta un cambio de la plana gerencial que se recibió el apoyo necesario para la realización de este proyecto.
- Adicionalmente, se pudo observar el poco interés y la poca concientización que se tiene con respecto a la seguridad de la información dentro del personal operativo, algo que resulta sorprendente teniendo en cuenta que, dentro de las diversas áreas, existen casos de personas con procesos judiciales debido a un intercambio no autorizado de credenciales.
- Por último, otro de los principales problemas hallados, fue la demora en la coordinación con el área de logística para la atención de las órdenes de compra, esto ha traído como consecuencia, la demora en la atención de riesgos graves que fueron identificados previamente por la organización debido a la falta de herramientas y recursos necesarios para su tratamiento.

7.2. Conclusiones

Luego de haber realizado el proyecto de fin de carrera en SERPOST se puede concluir lo siguiente:

- El apoyo de la alta gerencia para el diseño de este sistema de gestión fue imprescindible, debido a que fue necesaria su intervención para ayudar a concientizar a los jefes de área y dueños de los procesos a participar de las entrevistas de levantamiento de información y ayudó a que entendieran que el SGSI no solo busca proteger la información digital, sino toda la información crítica del negocio independientemente del medio que la contenga.
- Es necesario difundir las normas de seguridad existentes y establecer charlas de capacitación y concientización en toda la empresa, esto debido a la poca cultura de seguridad que existe en la organización, desde las planas gerenciales hasta el personal operativo, incluyendo al personal de seguridad, debido a que se ha detectado que existen controles normados; sin embargo, estos no son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas.
- Existe una clara necesidad en la organización de contratar personal especializado para dar soporte a los procesos involucrados en el SGSI, debido a que los recursos actuales no se dan abasto para atender los requerimientos de los usuarios lo cual en muchos casos se ha utilizado como excusa para realizar actos que afectan la seguridad de la información como el préstamo de credenciales de usuarios, uso de un correo para varias personas o la dejadez en la generación de respaldos de información del área.
- Es necesario mejorar la comunicación con el área de logística para acelerar los procesos de compra de aquellos activos que nos ayudaran en el tratamiento de riesgos detectados, especialmente, si estos riesgos son considerados altos o graves por la organización

7.3. Recomendaciones y trabajos futuros

- Debido a que existe una normativa que exige a SERPOST la implementación de un SGSI, que el alcance del SGSI de la organización es mayor al alcance del presente proyecto y que la organización no posee experiencia en la implementación de este sistema de gestión, se recomienda adquirir los servicios de una consultora que pueda guiar una implementación exitosa de la norma.
- Es recomendable evaluar la adquisición de una herramienta que les permita gestionar el SGSI de una forma más rápida y eficiente, incluyendo la gestión de los riesgos detectados en la organización.
- También, se recomienda establecer, como mínimo, reuniones mensuales del comité de seguridad de la información para dar un seguimiento adecuado a cada uno de los avances realizados en el sistema de gestión, así como ir aumentando de manera progresiva el alcance del mismo para lograr asegurar, a corto plazo, la información de toda la empresa.
- Se recomienda realizar un cambio en el organigrama de SERPOST, debido a que el actual oficial de seguridad de la información (OSI), no posee una independencia ni tiene el empoderamiento necesario para impulsar estos cambios en la organización, debido a ello, se depende mucho de los otros gerentes para la toma de decisiones lo cual puede demorar algunos procesos, adicionalmente, es necesario contemplar el rol del OSI en el cuadro de asignación de personal (CAP) de SERPOST para asegurar la continuidad del sistema de gestión y definir un personal estable debido a que la persona que está desempeñando el cargo lo realiza de manera temporal ya que, si bien tiene mucha disposición para el tema, tiene otras obligaciones en la empresa por la que no puede dedicarse a tiempo completo a velar por el correcto cumplimiento de estos temas.
- Es necesario que la organización asigne un presupuesto orientado a la implementación de los controles del SGSI, así como para las capacitaciones y charlas de concientización, los servicios de consultoría y las revisiones anuales que se darán para asegurar la continuidad del sistema.
- Debido a las deficiencias en la entrega de servicios detectadas en la empresa, se propone como un trabajo futuro, el diseño e implementación del marco ITIL v3 en la organización para la mejora de entrega de servicios y establecimiento de métricas que permitan monitorear los cambios propuestos.
- Adicionalmente, se recomienda evaluar el uso de COBIT 5.0 como marco de trabajo para la gestión del SGSI, de igual manera, se podría incluir la gestión de servicios de TI, según el enfoque de ITIL v3 mencionada en el punto anterior.
- También, se propone como trabajo futuro el diseño e implementación de un sistema de gestión de continuidad de negocio, debido a que no existe en la organización y es motivo de observación continua por parte de auditoria externa.
- Por último, considerando que la NTP ISO/IEC 27001:2008, está basada en la ISO/IEC 27001:2005 y que existe una nueva versión del año 2013, se propone como trabajo futuro, la actualización del sistema de gestión de seguridad de la información, una vez este sistema se haya implementado exitosamente en la empresa.

8. Referencias bibliográficas

Oficina Nacional de Gobierno Electrónico e Informática (ONGEI)
Portal de seguridad de información
Consultado en: 11/04/2013
http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552

INDECOPI
2013**. "**INDECOPI garantiza la seguridad de la información al obtener la Certificación ISO 27001". Noticia en página web. Consulta: 16 de junio de 2013.
http://www.indecopi.gob.pe/0/modulos/NOT/NOT_DetallarNoticia.aspx?PFL=0&NOT=612

BSI, ¿Qué son los sistemas de gestión?, 2013
Consultado en: 17/04/2013
http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/De-un-vistazo/Que-son-los-sistemas-de-gestion/

HALVORSON, Nick.
2008. "Information Risk Management: A Process Approach to Risk Diagnosis and Treatment". Information Security Management Handbook. 6th edition. Volume 2. USA: Auerbach Publications

OZIER, Will.
2004. "Risk Analysis and Assessment" Information Security Management Handbook. 5th edition. USA: Auerbach Publications

TUPIA, Manuel
2009. Principios de auditoría y control de sistemas de información.
PERÚ: Tupia Consultores y Auditores S.A.C.

PELTIER, Thomas R.; PELTIER, Justin; BLACKLEY, John
2005. Information Security Fundamentals. USA: Auerbach Publications

COBIT 5
Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa
ISACA, USA.
2012

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método
Ministerio de Hacienda y Administraciones Públicas, España
2012

OCTAVE – Information security risk evaluation
CERT, http://www.cert.org/octave/
2008.

ESCORIAL, Ángel
2012. "La gestión de riesgos impulse la credibilidad y la transparencia". Gerencia de Riesgos y Seguros. España, 2012, Primer cuatrimestre, No 112, pp. 86. 49-57.

CARLSOM, Tom
2008. "Understanding Information Security Management System". Information Security Management Handbook. 6th edition. Volume 2. USA: Auerbach Publications

ITGI; OGC
2008. “Alineando CobIT 4.1, ITIL v3 e ISO 27002 en beneficio del negocio ” USA: ITGI, ISACA, OGC y TSO
http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf

MOEN, Ronald D.; NORMAN, Clifford L.
2009, “The History of the PDCA Cycle” acta presentada en el séptimo congreso ANQ (Asian Network for Quality). Tokyo, 17 de septiembre de 2009. Consultada el 13 de junio de 2013.
http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf

AGUIRRE, David
2013, Entrevista1. Entrevista del 3 de mayo al Ingeniero Carlos Horna.

BARRAGÁN, Israel; INGRID, Góngora; MARTÍNEZ, Ericka
2011, Implementación de Políticas de Seguridad Informática para la M.I. Municipalidad de Guayaquil aplicando la norma ISO/IEC 27002. Tesis de grado. Ecuador: Escuela Superior Politécnica del Litoral.
http://www.dspace.espol.edu.ec/handle/123456789/21546

AMPUERO, Carlos
2011. Diseño de un Sistema de Gestión de Seguridad de Información para una Compañía de Seguros. Tesis para optar por el Título de Ingeniero Informático. Perú: Pontificia Universidad Católica del Perú.
http://tesis.pucp.edu.pe/repositorio/handle/123456789/933

KAZEMI, Mehdi; KHAJOUEI, Hamid; NASRABADI, Hashem
2012. “Evaluation of information security management system success factors: Case study of Municipal organization”.
AJBM - African Journal of Business Management.
Nigeria, 11 de abril, 2012, Vol. 6, No. 14, pp. 4982-4989
http://www.academicjournals.org/ajbm/pdf/pdf2012/11April/Kazemi%20et%20al.pdf

A Guide to the Project Management Body of Knowledge (PMBOK® Guide)
Project Management Institute
2013; Fifth Edition

OMG. BPMN Information Home.
Consultado el 06 de Junio de 2013
http://www.bpmn.org/

International Standard ISO/IEC 27000
Second Edition
Publicada el 01/12/2012

Estándar Internacional ISO/IEC 27001:2005
Primera Edición
Publicada el 15/10/2005

Estándar Internacional ISO/IEC 27002:2005
Primera Edición
Publicada el 15/06/2005

Estándar Internacional ISO/IEC 27003:2010
Segunda edición
Publicada el 01/02/2010

Estándar Internacional ISO/IEC 27005:2011
Segunda edición
Publicada el 01/06/2011

Norma Técnica Peruana ISO/IEC 27001:2008
INDECOPI
Publicada el 2008-12-12

Norma Técnica Peruana ISO/IEC 17799:2005
INDECOPI
Publicada el 2007-01-22

RM-246-2007-PCM
Presidencia de Consejo de Ministros
Fecha de Promulgación: 22 de agosto del 2007

RM-197-2011-PCM
Presidencia de Consejo de Ministros
Fecha de Promulgación: 14 de julio del 2011

RM-129-2012-PCM
Presidencia de Consejo de Ministros
Fecha de Promulgación: 23 de mayo del 2012

Resolución 007-2011/CNB-INDECOPI
Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias
Fecha de Promulgación: 30 de marzo del 2011