PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UNA EMPRESA INMOBILIARIA ALINEADO A LA NORMA ISO/IEC 27001:2013

Tesis para optar por el Título de Ingeniera Informática, que presenta la bachiller:

Zully Isabel Justino Salinas

ASESOR: Moisés Villena Aguilar

Lima, Febrero de 2015

Agradecimientos

A mis padres, por su incondicional apoyo a lo largo de mi carrera universitaria.

A mi asesor, por sus recomendaciones y consejos.

Al grupo K. P. S., por su compañía.

A Diego.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

1 Problemática

Hoy en día, muchas empresas invierten en Tecnologías y Sistemas de información con el fin de satisfacer las necesidades del negocio y tener mejor control sobre sus operaciones. Desde una perspectiva de negocios, los sistemas de información forman parte de una serie de actividades que agregan valor para adquirir, transformar y distribuir la información que los gerentes pueden usar para mejorar la toma de decisiones, el desempeño de la organización y, en última instancia, incrementar la rentabilidad de la empresa. [LAUDON, 2012]

De acuerdo a lo mencionado, la información, tanto digital como física, cumple un papel muy importante ya que actúa como activo principal y genera valor económico real para una organización. Si una empresa no administra, protege o asegura adecuadamente su información estará expuesta a riesgos que perjudicarán la continuidad de su negocio. Es por ello, que toda información debe ser protegida, para que se encuentre accesible en tiempo y forma o, desde el punto de vista de la Seguridad de información, conserve sus características de confidencialidad, integridad y disponibilidad.

En este contexto, pese a que en la última década, algunas empresas han puesto énfasis al tema de seguridad de información, muchas otras han tenido problemas con respecto a este tema; es así como los riesgos que enfrenta una organización se materializan, tales como fraudes, fuga y pérdida de información, exposición de información confidencial, entre otros. Según ISACA, a nivel global, el 22% de las empresas estudiadas habían sido víctimas de ataques a su seguridad y el 21% enfrentaba problemas con dispositivos, en otras palabras, uno de cada cuatro empresas sufren problemas de seguridad de información. Además en Latinoamérica, se encontró que tres de cada diez empresas, experimentó una brecha de seguridad y el 16% ha enfrentado problemas de seguridad en dispositivos móviles. [ISACA, 2012a] En este entorno, se debe saber que para solucionar estos problemas, cada organización tendrá sus propias necesidades y/o requerimientos de seguridad.

Tomando el caso de una empresa del sector inmobiliario, cuyo negocio principal se resume en aquel que identifica un conjunto de terrenos o lotes, de los cuales escogerán los más adecuados para luego agregarles valor mediante la ejecución de obras, como la construcción de edificaciones y de habilitación urbana, para ponerlo a disposición y venderlo a los clientes. Del mismo modo, detrás de todo este proceso principal, están los procesos de soporte, los cuales se resumen en el planeamiento estratégico, el cuál define los lineamientos para desarrollar los proyectos inmobiliarios; la relación con inversionistas, en el que se captan y se recaudan fondos para invertir en dichos proyectos y finalmente el servicio post-venta el cual se les brinda a los clientes. Toda la información que se maneja a lo largo de los procesos, tanto la operativa, financiera y la de gestión, es necesaria para la toma de decisiones gerenciales

Como se puede observar, hay una gran cantidad de información que una inmobiliaria tiene la necesidad de proteger. Esto es porque, desde un enfoque externo, se ha detectado la amenaza de fuga de información, así como ataques que pueden comprometer el valor comercial de ésta, un ejemplo de lo que sucede actualmente con la información de los clientes, inversionistas, estrategias de marketing, estudios de mercado, de proyectos y principalmente la información de los terrenos vacíos que tienen como reserva. Esto se debe a que en el Perú la competencia en este sector se ha incrementado, y éstas buscan colocar sus productos en las condiciones más atractivas, lo que podría repercutir fuertemente en sus inversiones. Desde un enfoque interno, existe el riesgo de no contar con información precisa, correcta, confiable y oportuna, esto debido a que se encuentra dispersa, no es uniforme, ni homogénea; asimismo existe el riesgo de que la infraestructura de TI no soporte la operación ni el crecimiento esperado de la organización.

Esta misma situación no sólo ocurre en Perú, hablando en términos de Gobierno de seguridad de información, los hallazgos de un estudio realizado en Australia a 40 organizaciones del sector inmobiliario resaltan la necesidad que tienen las empresas inmobiliarias para entender la importancia de los facilitadores de gobierno adecuado, sobretodo entender que la seguridad de información no sólo es costo o un tema que sólo compete a TI, sino que puede facilitar el intercambio económico y entregar beneficios reales al negocio. Asimismo, se enfatiza que un entorno de seguridad de información eficaz no sucede de la noche a la mañana y que requiere

de estrategias, políticas y objetivos que se alinean con las necesidades del negocio de la organización. [DEEPA, KIM y SAMEERA, 2013]

Todo esto supone que se necesita una adecuada gestión de la seguridad de información, el cual no solo involucra al área de TI sino que también es imprescindible incluir a la alta dirección, pues su participación es clave para una gestión eficiente de la información.

Por tal motivo, en el presente proyecto de fin de carrera, se pretende dar solución mediante la administración de la seguridad de información en una empresa del sector inmobiliario, cuyo objetivo será gestionar de manera eficiente la información, y desde el punto de vista de la alta dirección, permitir obtener una visión global del estado de los sistemas de información sin caer en detalles técnicos, además de observar las medidas de seguridad aplicadas y los resultados obtenidos, para finalmente tomar las mejores decisiones estratégicas para la organización.

1.1 Objetivo general

Diseñar un sistema de gestión de seguridad de la información para una empresa del sector inmobiliario tomando como base las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013.

1.2 Objetivos específicos

1. Elaborar la documentación exigida por la norma ISO/IEC 27001:2013.
2. Modelar los procesos de negocio críticos de la unidad de negocio Vivienda.
3. Definir una metodología para la valorización de activos.
4. Definir una metodología de gestión de riesgos.
5. Realizar un mapa de riesgos de los procesos del alcance.
6. Identificar los controles asociados a los riesgos identificados, empleando la norma ISO/IEC 27002:2013.
7. Elaborar el documento de declaración de aplicabilidad.

1.3 Resultados esperados

- Resultado 1: Documentación requerida por la norma ISO/IEC 27001, de acuerdo a los lineamientos específicos en la norma ISO/IEC 27003.
- Resultado 2: Mapa de procesos de negocio de la unidad de negocio Vivienda.
- Resultado 3: Relación de activos de información más relevantes.
- Resultado 4: Metodología de Gestión de Riesgos.
- Resultado 5: Mapa de riesgos.
- Resultado 6: Lista de controles según la ISO/IEC 27002:2013.
- Resultado 7: Documento de declaración de Aplicabilidad.

2 Herramientas, métodos, metodologías y procedimientos

A continuación se presenta el siguiente cuadro que relaciona las herramientas y metodologías que se usarán para hallar cada resultado esperado.

Resultados esperado	Herramientas a usarse
1) Resultado 1: Documentación requerida por la norma ISO/IEC 27001.	**ISO/IEC 27001 e ISO/IEC 27003** Ambos son estándares de la familia ISO 27000 que contempla normas de Gestión de Seguridad de información. **EDT Estructura de Desglose del trabajo.** El proceso de subdividir los entregables y el trabajo del proyecto en componentes más pequeños y más fáciles de manejar. [PMI, 2013]
2) Resultado 2: Mapa de procesos de negocio de la unidad de negocio Vivienda.	**Business Process Modeling Notation** o también llamada BPMN, es una notación gráfica estandarizada que permite el modelado de procesos de negocio, en un formato de flujo de trabajo. **Bizagi Process Modeler** Software gratuito que soporta BPMN 2.0.
3) Resultado 3: Relación de activos de información relevantes.	**ISO/IEC 31000:2009** Es un estándar enfocado específicamente a la Gestión de riesgos, éste puede ser aplicado para toda una organización, en sus distintas áreas y niveles, así como funciones, proyectos y actividades específicas.
4) Resultado 4: Metodología de Gestión de Riesgos.	
5) Resultado 5: Mapa de riesgos.	
6) Resultado 6: Lista de controles según la ISO/IEC 27002.	**ISO/IEC 27002:2013** Código de buenas prácticas para la gestión de Seguridad de la Información. Es un estándar de la familia ISO 27000 que contempla los requisitos para la implementación del Sistema de Gestión de Seguridad de Información.
7) Resultado 7: Documento de declaración de Aplicabilidad.	

Tabla 1. Mapeo de resultados esperados y herramientas o metodologías.

2.1 Herramientas

2.1.1 BPMN 2.0

Se trata de un estándar de la OMG (Object Management Group). La notación para el modelado de procesos de negocio, BPMN por sus siglas en inglés, es una notación gráfica que diagrama las actividades de un proceso de negocio. Esta

notación representa de extremo a extremo el flujo de proceso de negocio y se ha diseñado específicamente para coordinar la secuencia de procesos y mensajes que fluyen entre los diferentes participantes del proceso en un conjunto relacionado de actividades. [OMG, 2012]

Esta herramienta será muy útil para el resultado esperado 3, mapa de procesos de negocios, ya que maneja muchos elementos con los que se puede representar todo tipo de procesos, desde procesos de negocio hasta procesos de TI, además introduce el concepto evento para simplificar los diagramas.

2.1.2 Guía PMBOK versión 5

PMBOK (A guide to the Project Management Body of Knowledge) es una colección y áreas de procesos generalmente aceptadas como las mejores prácticas dentro de la gestión de proyectos que fue publicada por el PMI (Project Management Institute).
En la versión actual, se introducen dos cambios; el primer cambio consiste en reconocer una nueva área de conocimiento, la Gestión de los Interesados (Stakeholders).

Algunas de las herramientas y técnicas que se describieron anteriormente, son elementos que servirán a lo largo del desarrollo del proyecto.

2.1.3 ISO 27001:2013

Este estándar fue preparado por el comité técnico conjunto ISO/IEC JTC1, Tecnología de Información, Subcomité SC 27, Técnicas de seguridad de TI. Esta norma en su segunda edición, cancela y reemplaza a la primera (ISO/IEC 27001:2005) la cuál ha sido revisada. La norma ha sido preparada para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. [ISO 27001, 2013]

Para el presente proyecto, se usará algunos puntos de la norma para diseñar el Sistema de Gestión de Seguridad de información, en adelante SGSI, en una empresa inmobiliaria.

2.1.4 ISO 27002:2013

Se trata de la segunda edición de la norma, la cual reemplaza y cancela el ISO/IEC 27002:2005. Con 14 secciones y 113 controles, esta norma contiene el Código para la práctica de la gestión de la seguridad de la información (previamente BS 7799 Parte 1 y la norma ISO/IEC 17799). Este estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados. [ISO 27002, 2013]

2.1.5 ISO 27003:2010

Directrices para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Es el soporte de la norma ISO 27001. [ISO 27003, 2010]

Esta norma servirá de ayuda y guía para realizar el diseño de un Sistema de Gestión de Seguridad de Información que describe el estándar ISO/IEC 27001, a través de algunas de sus cláusulas.

2.1.6 ISO/IEC 31000:2009

Esta norma internacional fue preparada por el Grupo de trabajo de Técnica en Gestión de riesgos. El estándar establece un número de principios que necesitan ser satisfechos por una gestión de riesgos eficaz; asimismo, recomienda a las organizaciones el desarrollo, implementación y una mejora continua de un marco cuyo propósito es integrar los procesos de la gestión de Riesgos dentro del gobierno de la organización. [ISO 31000, 2009]

Para el proyecto se utilizará y seguirá el esquema de procesos de la gestión de riesgos enfocado a seguridad de información que presenta la norma.

2.2 Métodos y procedimientos

2.2.1 Revisión de documentos

Revisión estructurada de los documentos del proyecto, incluyendo los planes, asunciones, archivos de proyectos pasados, y otra información. La calidad de los planes, la consistencia entre dichos planes y los requerimientos y asunciones del proyecto pueden ser indicadores del riesgo en el proyecto. [PMI, 2013]

Esta técnica permitirá generar un proyecto claro y ordenado con relación a la consistencia de los entregables y documentos realizados.

2.2.2 Técnicas de recopilación de información

Algunas de las técnicas de recopilación de información que menciona la Guía PMBOK versión 5, son las siguientes:

- Tormenta de ideas - Si se emplea esta técnica es recomendable utilizar un moderador.
- Técnica Delphi – Consenso de expertos. Participación anónima.
- Entrevistas – A expertos en temas relacionados con el proyecto.
- Identificación de las causas raíz.
- Análisis FODA – Fortalezas, Oportunidades, Debilidades, Amenazas. [PMI, 2013]

Con estas técnicas, se podrá recoger información de la empresa inmobiliaria, en la unidad de negocio de Vivienda. Además se podrá deducir la secuencia de actividades que están contenidas en los procesos de negocio.

2.2.3 Técnicas de diagramación

Las técnicas de diagramación de riesgos pueden incluir:

- Diagramas de causa y efecto, estos son conocidos como diagramas de Ishikawa y son útiles para identificar las causas de los riesgos.
- Diagramas de flujo o de sistemas, muestran cómo se interrelacionan los diferentes elementos de un sistema, y el mecanismo de causalidad.
- Diagrama de influencias, son representaciones gráficas de situaciones que muestran influencias causales, la cronología de eventos y otras relaciones entre variables y los resultados. [PMI, 2008]

Esta técnica se usará en algunos de los resultados esperados, ya que ayudarán a ordenar mejor las ideas.

2.3 Metodologías

2.3.1 Ciclo de mejora continua o Deming

El ciclo de Deming o más conocido como PDCA (Plan-Do-Check-Act) es un proceso metodológico desarrollado por Shewart y Deming para abordar los proyectos de mejora sobre procesos propios, externos e internos. Hoy en día, muchas normas ISO y estándares basan sus requisitos en este ciclo de mejora, y establecen que los Sistemas de Gestión se organicen siguiendo las siguientes 4 fases:

* Planificar (Plan), en la que se establecen las labores a llevar a cabo para implantar dicho sistema, indicando responsables y plazos, asimismo se establecen políticas de gestión y los objetivos.
* Hacer (Do), en esta fase se llevan a cabo las acciones planificadas anteriormente, en el cual se incluyen la formación, la comunicación, documentación, procesos críticos, etc. Una vez que las actividades se han puesto en marcha y están en funcionamiento, se llega a la tercera fase del ciclo.
* Verificar (Check), se evalúan los resultados reales conseguidos y se comparan con los objetivos establecidos en la planificación. Además, se debe determinar indicadores para la medición de objetivos.
* Mejorar (Act), en esta fase se obtiene un grado de rendimiento superior al anterior. La alta dirección se encarga de revisar los objetivos previstos con los resultados reales, si se alcanzó lo planificado, los cambios son sistematizados y normalizados. Además, se evalúa todo el proceso desde el comienzo de ciclo, pasando por todas las fases, y estableciendo acciones necesarias para mejorarlo, dando comienzo nuevamente a la fase PLAN. [PDCA, 2013]

El proyecto de Diseño de un Sistema de Gestión de Seguridad de Información incluye dos de estas fases, la fase de Planificar y la fase Hacer. Según el estándar ISO/IEC 27001:2013, la fase de planificación consiste en especificar acciones para hacer frente a los riesgos e identificar oportunidades; y consecuentemente proceder a evaluarlos y gestionarlos. En la fase Hacer, el estándar indica que la organización

debe determinar y proveer de los recursos necesarios para establecer, implementar y mantener un sistema de Gestión de Seguridad de la Información; además, las personas que trabajen dentro de la organización deben ser conscientes de las políticas de seguridad de información, así como su contribución a la efectiva Gestión de Seguridad de información.

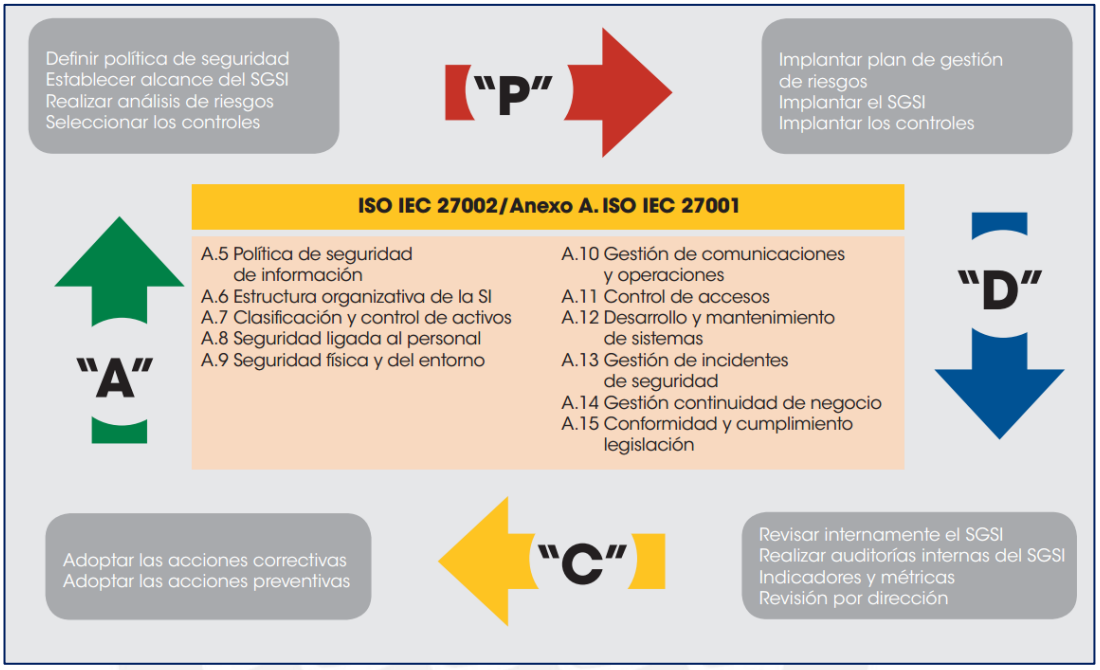


Figura 1. Ciclo PDCA de mejora continua
Fuente: AENOR

3 Alcance

Tal y como se ha visto en la problemática, una empresa presenta un universo de problemas con respecto a la seguridad de información en los diferentes procesos de negocio. Para el presente proyecto, el problema estará enfocado a la deficiente gestión de seguridad de información de una empresa inmobiliaria para la unidad de negocio de vivienda, el cual es una de las unidades más complejas debido a los diversos procesos de negocio que se gestionan. Los procesos del alcance serán:

* Proceso de Reserva Territorial
* Proceso de Desarrollo de Proyectos
* Proceso de Ejecución de obras
* Proceso de Ventas

* Proceso de Cobranzas
* Proceso de Tecnología de información

3.1 Limitaciones

Como limitaciones del proyecto de investigación se puede considerar:

- La ausencia de documentos o documentación desactualizada de algunos o todos los procesos del alcance.
- Inconsistencia de la información recopilada de la empresa y los procesos de negocio documentados.
- Por políticas de la empresa, no entregarán información que servirá para el desarrollo del proyecto.

Un obstáculo que se puede presentar en el proyecto es la indisponibilidad del personal de la empresa inmobiliaria encargada de los procesos, esto dificulta el desarrollo de trabajo en campo.

3.2 Riesgos

Los riesgos que pueden afectar y amenazar el desarrollo del Proyecto de fin de grado, se presentan a continuación:

Riesgo identificado	Impacto en el proyecto	Medidas correctivas para mitigar
- Restricciones para acceder a la información de la empresa inmobiliaria.	ALTO	Firmar un acuerdo de confidencialidad con la empresa que permita acceder a la información.
- Desconocimiento de las herramientas.	MEDIO	Investigación constante de las herramientas a utilizar, mediante tutoriales u otros medios.
- Retrasos en el proyecto, entregables entregados a destiempo.	ALTO	Planificación y organización de actividades.
- Algunos de los entregables no cumplen con la aceptación para la presentación final.	ALTO	Enviar permanentemente los avances al asesor para que puedan ser corregidos.

- No cumplir con los objetivos específicos del proyecto, además de no terminar con el proyecto en el tiempo estimado.	ALTO	Balancear esfuerzo vs tiempo en cada entregable.
- Inconsistencia entre el entregable presentado por el tesista y las revisadas por el asesor.	ALTO	Más reuniones personales y/o comunicación por correo electrónico con el asesor.
- El tesista o el asesor pueden quedar incapacitados, temporal o permanentemente y no puede seguir apoyando en el desarrollo del proyecto.	ALTO	Buscar otros mecanismos de comunicación. En el caso del que el asesor este incapacitado, comunicar a los profesores del curso, para obtener una reasignación de asesor, de tal forma que se comunique sobre todo el desarrollo del proyecto y el alcance.
- Recursos tecnológicos o bibliográficos no disponibles.	ALTO	Coordinar a tiempo con los proveedores de recursos para tenerlos disponibles en cualquier momento.
- Pérdida de todos los entregables previa presentación final.	ALTO	Realizar al menos tres backups de diferentes maneras de los entregables.
- Retraso en las aprobaciones y correcciones de los entregables del proyecto.	ALTO	- Envío de entregables con cinco días de anticipación como máximo al día de entrega. - Comunicarse constantemente con el asesor.

Tabla 2. Cuadro de riesgos que afectan al Proyecto de fin de grado.

4 Justificación y viabilidad del proyecto

4.1 Justificativa

Como se revisó en la problemática, la información de los proyectos, específicamente la lista de terrenos en reserva y perfil de proyecto inmobiliario que contiene el análisis de factibilidad del futuro proyecto (estrategias, planes, estudios); fichas que contienen la información de inversionistas, clientes y proveedores (datos personales, cuentas bancarias, DNI, sustentos bancarios o procedencia de fondos, entre otros) son valiosos activos de los que depende el buen funcionamiento de la organización, por ello es indispensable mantener su integridad, confidencialidad y disponibilidad para alcanzar los objetivos del negocio. Para proteger la información de la empresa inmobiliaria de cualquier amenaza y/o riesgos es necesario

conocerlos de manera adecuada. El presente proyecto se realizará para contribuir con algunos controles de seguridad basados en la evaluación de riesgos, que puedan ser usados por una inmobiliaria que tenga la unidad de negocio de vivienda como actividad crítica, con el fin de reducir las amenazas o mitigar riesgos de seguridad hasta considerarlos como aceptable para la organización.

Con este proyecto, la entidad dará un primer paso para poder certificarse con el estándar ISO/IEC 27001:2013, el cual contribuirá a mejorar la competitividad en el mercado, diferenciando a la empresa con otras de su sector, haciéndola más fiable e incrementando su prestigio. Un certificado mejora la imagen y confianza de la empresa con sus clientes, proveedores y socios que, poco a poco, exigen certificación.

4.2 Análisis de viabilidad del proyecto de tesis

El diseño de un Sistema de Gestión de Seguridad de la información como el diseñado en el siguiente proyecto que estará basado en la norma ISO/IEC 27001:2013, es viable para la empresa del sector inmobiliario de la cual se recolectará la información, puesto que cuenta con los suficientes recursos económicos para que en un futuro próximo se pueda aplicar los controles diseñados en el proyecto.

En cuanto a viabilidad temporal, el proceso comenzará a partir de cero y se extenderá en el tiempo en función de las necesidades de protección y los recursos de la organización. Aproximadamente, un proyecto de diseño de un SGSI tiene una duración de 4 a 6 meses, dependiendo de las necesidades de la inmobiliaria.

CAPÍTULO 2

1 Marco teórico

En esta sección se describirán los conceptos necesarios para la comprensión del documento.

1.1 Normas y regulaciones

- **LEY Nº 29733 - LEY DE PROTECCIÓN DE DATOS PERSONALES**

En el 2011, se promulgó la ley de protección de datos personales en el Perú, la cual tiene como objetivo garantizar el derecho fundamental a la protección de los datos personales, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconoce. En el 2013, se aprobó esta ley y entró en vigencia en mayo del mismo año.

Consta de 7 títulos y 40 artículos que describen los principios, el tratamiento de datos personales, los derechos del titular, obligaciones del titular y el encargado del banco de datos, la autoridad nacional de cumplimiento de la ley y finalmente, las infracciones y sanciones administrativas ante la presunta comisión de actos contrarios a lo dispuesta a ley [CONGRESO DE LA REPÚBLICA DEL PERÚ, 2011].

Toda información relativa a una persona se le conoce como dato personal. La norma se aplica a los datos personales contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realice en el territorio nacional. El sentido de esta ley es que toda información personal no sea usada indiscriminadamente sin el consentimiento de la persona, salvo se establezcan determinadas excepciones como la investigación de un delito.

El ente regulador de esta ley es la Dirección General de Protección de Datos Personales o Autoridad Nacional de Protección de Datos Personales cuya función es la de cumplir y hacer cumplir la normatividad vigente en materia de

protección de datos personales. Sus funciones son administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras. [APDP, 2013]

1.2 Conceptos relacionados al problema

A continuación se definirá algunos conceptos relacionados al problema para la correcta comprensión del documento.

- **Procesos de negocio**

Se define como procesos de negocio al conjunto de tareas y comportamientos lógicamente relacionados que las organizaciones desarrollan a través del tiempo para producir resultados de negocios específicos y a la manera particular en la cual se organizan estas actividades [LAUDON, 2012].

- **Alta dirección**

Dentro de los niveles de una empresa, la alta dirección es la encargada de tomar las decisiones estratégicas más importantes relacionadas con productos y servicios, esto garantiza el desempeño financiero de la empresa [LAUDON, 2012].

- **Infraestructura de TI**

Se define a la infraestructura de TI de una empresa como los recursos compartidos que proporcionarán la base, sobre la cual una organización construirá sus sistemas de información específicos. Por ello, es necesario que cada institución diseñe y opere cuidadosamente su infraestructura, de tal manera que cuente con el conjunto de servicios tecnológicos requeridos para el desarrollo de sus procesos [LAUDON, 2012].

La infraestructura incluye inversiones en hardware, software y servicios, como consultoría, soporte y mantenimiento, que se comparten a través de toda la empresa.

- **Data Center**

Tal como su nombre indica, se trata de un “centro de datos”, es un espacio reservado en el que las empresas mantienen y operan la mayor parte de la infraestructura de TI que apoya su negocio. Esto sería los servidores y equipos de almacenamiento en los que se ejecutan el software de aplicación y se almacenan datos y contenidos.

Por definición, es la instalación de computadores diseñados para el uso continuo por varios usuarios; equipada con hardware, software, periféricos de acondicionamiento de potencia y copias de seguridad, equipos de comunicación, sistemas de seguridad, entre otros. [TECH, 2010]

- **Sistemas empresariales**

Los sistemas empresariales integran los procesos de negocios clave de una empresa en un solo sistema de software con el propósito de que la información fluya a través de la organización, mejorando la coordinación, la eficiencia y la toma de decisiones. El software empresarial se construye en base a un conjunto de módulos de software integrado y en una base de datos central común [LAUDON, 2012].

- **Riesgo**

Según la RAE, el riesgo se define como contingencia o proximidad de un daño, o como cada una de las contingencias que pueden ser objeto de un contrato de seguro [RAE, 2001].

Según ITIL, el riesgo se presenta como una incertidumbre en el resultado de la aplicación de un servicio o proceso, el cual está relacionado a la probabilidad de que un evento se materialice alterando su normal ejecución [TUPIA, 2013b]

- **Seguridad de la información**

La seguridad de información se caracteriza por la preservación de la confidencialidad, asegurando que la información sea accesible sólo por aquellos que están autorizados; la integridad, salvaguardando la exactitud de la

información en su procesamiento; y finalmente su disponibilidad, asegurando que los usuarios tengan acceso a la información y a los activos asociados cuando sean requeridos [VILLENA, 2006]

Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla criterios de:

- Confidencialidad, garantía de que la información sea accedida por las personas convenientemente autorizadas.
- Integridad, la información debe mantenerse permanentemente correcta, compleja y protegida.
- Disponibilidad, la información debe estar disponible para su uso, cuando se lo requiera. También se considera como parte de la disponibilidad, la rapidez con que se puede ofrecer servicios o realizar operaciones. [TUPIA, 2013a]

1.3 Conceptos relacionados a la propuesta de solución

- **Sistema de Gestión de Seguridad de Información (SGSI)**

Este sistema se fundamenta en la norma UNE-ISO/IEC 27001:2007, es parte del sistema gerencial general, está basado en un enfoque de riesgo comercial para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de información; sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o ciclo Deming, o más conocido como PDCA (Plan-Do-Check-Act), asimismo se tiene su fundamento en la norma UNE-ISO/IEC 27002:2009 que recoge una lista de controles necesarios para lograr los objetivos de seguridad de información. El SGSI está diseñado para asegurar una selección de controles de seguridad que protejan los activos de información y den confianza a las partes interesadas. [AEC, 2012]

El diseño e implementación del SGSI de una organización está influenciado por las necesidades y objetivos del negocio, requisitos de seguridad, procesos, tamaño y estructura de la organización. Se espera que éstos y sus sistemas de soporte cambien a lo largo del tiempo, así como las situaciones simples requieran soluciones SGSI simples.

Figura 2. Esquema del Sistema de Gestión de Seguridad de Información ISO 27001
Fuente: Normas.ISO.com

- **BMIS (Business Model for Information Security)**

Este modelo tiene un enfoque integral y orientado a los negocios de gestión de seguridad de la información. Establece un lenguaje común para referirse a la protección de la información y permite a los profesionales examinar la seguridad desde la perspectiva de los sistemas, creando un entorno donde la seguridad se puede gestionar de manera integral, permitiendo que los riesgos reales sean abordados.

El BMIS se compone de cuatro elementos y seis interconexiones dinámicas, asimismo puede ser visto como un modelo tridimensional, mejor visualizada como pirámide. [ISACA, 2013b]

Elementos:

- Organización
- Personas
- Procesos
- Tecnología

Interconexiones dinámicas

- Cultura
- Arquitectura
- Gobierno
- Penetración
- Habilitación y soporte
- Factores humanos

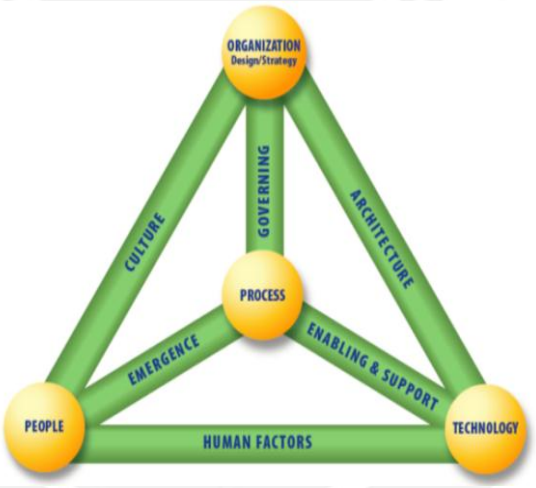


Figura 3. Esquema del Modelo de negocio para la Seguridad de Información
Fuente: www.isaca.org

- **Gobierno de la Seguridad de Información**

El Gobierno Corporativo consiste en un conjunto de políticas y controles internos por los cuales las organizaciones, independientemente de su tamaño y forma, son dirigidos y administrados. El Gobierno de Seguridad de Información es un subconjunto del programa general de gobierno de una organización, el cual incluye los elementos necesarios para brindar a la alta dirección la certeza de que su gestión e intención se reflejan en la situación de seguridad de la organización cuando se hace uso de un enfoque estructurado para implementar un programa de seguridad [ITGI, 2008]. El objetivo de este programa es

desarrollar, implementar y gestionar un plan de Seguridad de Información para alcanzar los cinco resultados básicos identificados en el Gobierno de Seguridad de Información los cuales se alinean a los dominios o componentes del Gobierno de TI:

- Alineamiento estratégico, el cual asegura que TI permita y apoye el logro de objetivos del negocio. La alineación estratégica de la seguridad de información con las estrategias de negocios para cumplir con los objetivos organizacionales.
- Entrega de valor, el cual asegura que TI y la empresa cumplan con sus responsabilidades de gestión de valor. Entrega de valor mediante la optimización de inversiones en seguridad de información en apoyo a los objetivos de negocio.
- Gestión de Riesgos, el cual asegura que existan los marcos de referencia apropiados y que estén alineados a los estándares relevantes. Administrar riesgos a través de la ejecución de medidas apropiadas para mitigar riesgos y reducir el posible impacto de los recursos de información a un nivle aceptable.
- Gestión de recursos, asegurar que TI tenga recursos suficientes, competentes y capaces de ejecutar los actuales y futuros objetivos estratégicos y mantenerse al día con las demandas del negocio. Administrar los recursos mediante el uso del conocimiento y estructura de la seguridad de información con eficiencia y eficacia.
- Medición del desempeño, asegurar que la empresa apoye las metas y objetivos de TI y que se establezcan mediciones en colaboración con los grupos de interés. Esto se realiza a través de la medición, monitoreo y reporte de las métricas de gobierno de seguridad de información para asegurar el logro de los objetivos organizacionales.

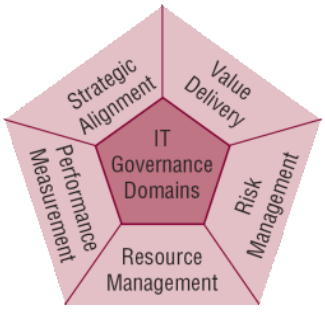


Figura 4. Dominios del Gobierno de TI
Fuente: Systemi.ca

Para lograr un efectivo Gobierno de Seguridad de Información, la Gerencia deberá establecer y mantener un marco para guiar el desarrollo y mantenimiento de un programa integral de Seguridad de información. El marco de gobierno generalmente consiste en:

- Una estrategia integral de Seguridad de información alineada a los objetivos de TI y de negocio de la organización.
- Una efectiva estructura organizacional de seguridad de información carente de conflictos de intereses con la autoridad y recursos apropiados.
- Políticas de seguridad de información que abordan cada aspecto de la estrategia, los controles y la regulación.
- Un conjunto de estándares de Seguridad de Información para asegurar que los procedimientos y directrices cumplan con cada política.
- Procesos de monitoreo específicos de la empresa, para asegurar el cumplimiento y proporcionar una retroalimentación continua eficaz.
- Un proceso que asegure la continua evaluación y actualización de las políticas de seguridad de información, estándares y procedimientos de la organización.
- Implementación de una efectiva metodología de evaluación de riesgos para la seguridad de información.

En la figura 5. se muestra las relaciones y los participantes involucrados en el desarrollo de una estrategia de seguridad alineada a los objetivos del negocio. La estrategia de negocio ofrece una de las entradas en la gestión de riesgos y la seguridad de información para facilitar la alineación. El equilibrio de las entradas se deriva de la determinación del estado deseado de seguridad en comparación con el estado actual, asimismo, se deben incluir los procesos de negocio, así como los resultados de la evaluación de riesgos y el análisis de impacto para determinar los niveles y prioridades de protección.

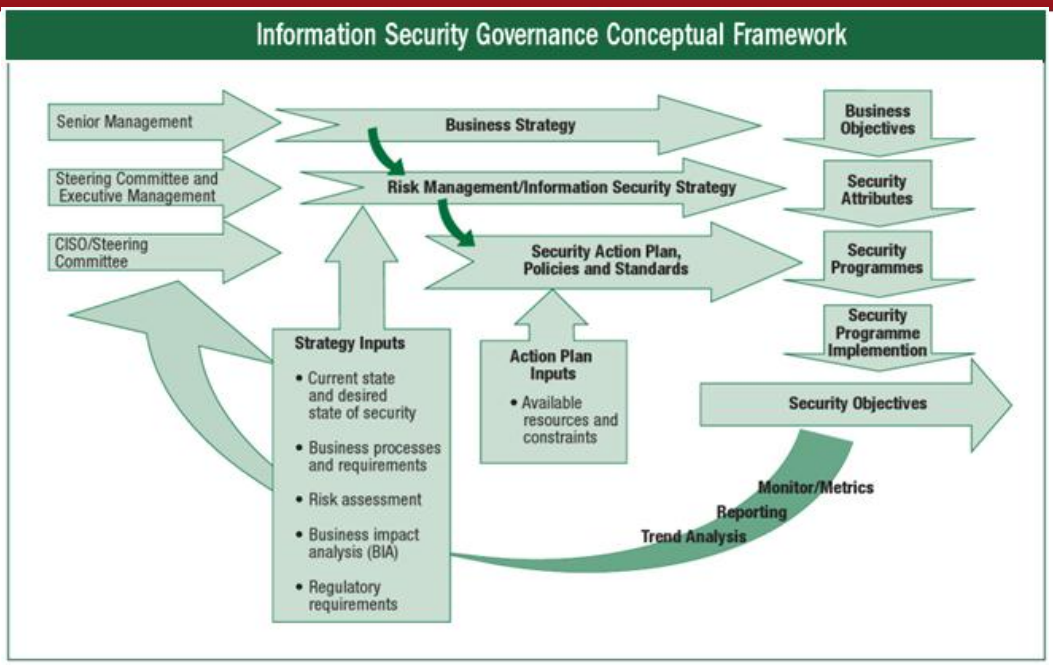


Figura 5. Marco conceptual del Gobierno de la Seguridad de Información
Fuente: ITGI, 2008

1.4 Otros conceptos

- **COBIT 5.0**

Se trata de un marco de gobierno de las Tecnologías de Información, desarrollado por ISACA, que proporciona una serie de herramientas a la gerencia con el fin de conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio, además permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías en toda la organización. COBIT 5 toma como base el modelo relacional BMIS (Business Model for Information Security), el cual presenta un enfoque integral y orientado al negocio para la gestión de la seguridad de información. Dentro de la familia de productos de COBIT 5 se encuentran guías habilitadoras y guías profesionales.

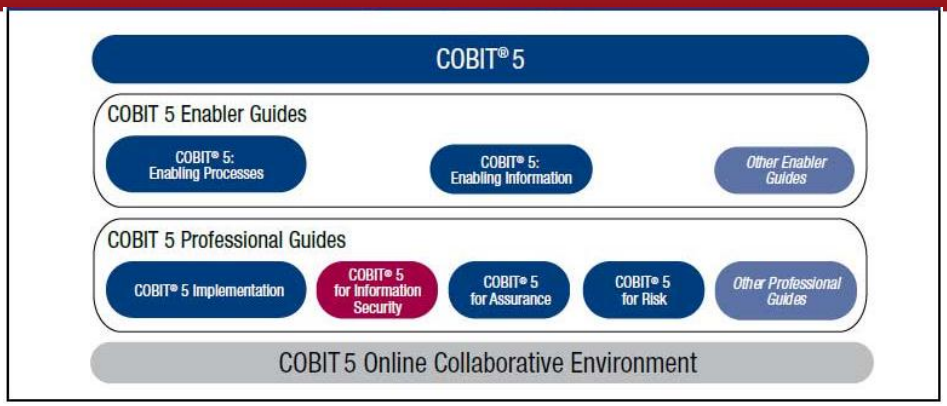


Figura 6. Familia de Productos de COBIT 5
Fuente: ISACA, 2012

- **COBIT 5 for Information Security**

Se trata de una guía específica para profesionales de la seguridad de información y otros interesados. Presenta una visión extendida del marco COBIT 5, que explica cada uno de sus componentes desde la perspectiva de seguridad y propone una visión del gobierno y la gestión de seguridad de la información mediante una guía detallada para implementarla y mantenerla, como parte de políticas, procesos y estructuras de la organización.

Dentro de su contenido, se tiene:

- Directrices sobre los principales controladores y beneficios de la seguridad de información para la organización.
- Aplicación de los principios de COBIT 5 por parte de los profesionales de seguridad de la información.
- Mecanismos e instrumentos para respaldar el gobierno y la gestión de la seguridad de información en la organización.
- Alineamiento con otros estándares de seguridad de la información.

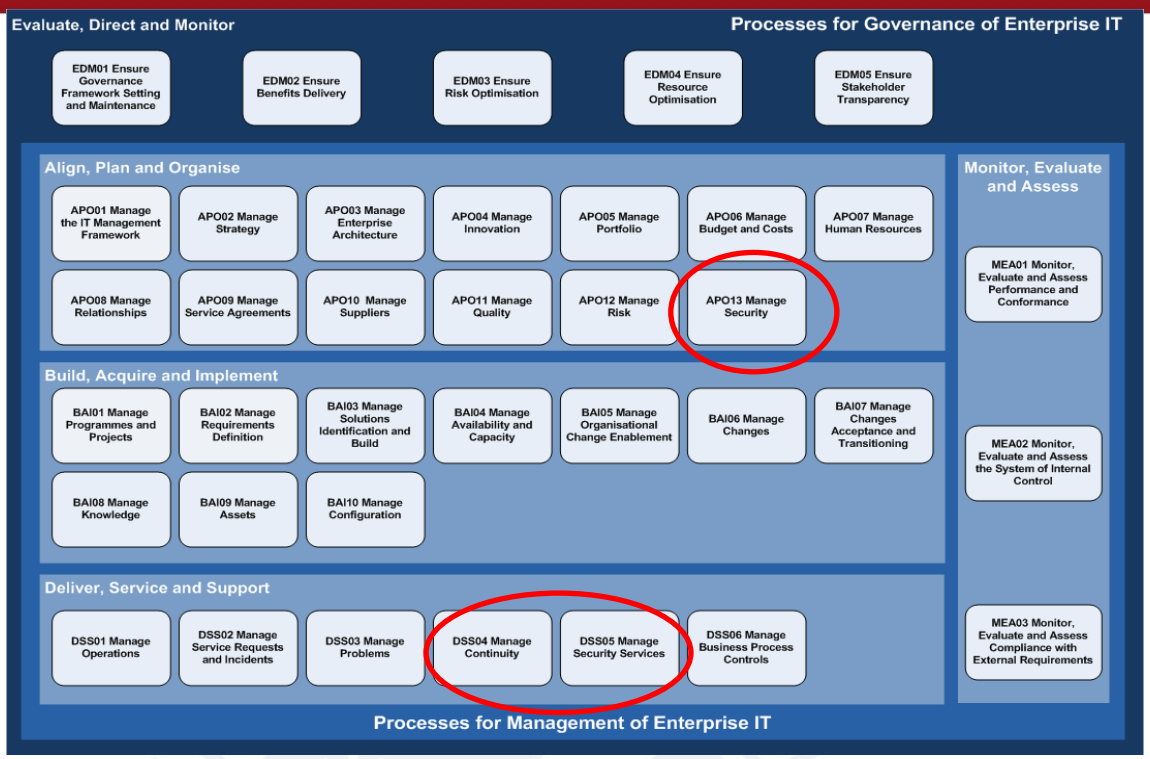


Figura 7. Procesos habilitadores de COBIT 5
Fuente: ISACA, 2012

ISACA define seguridad de información como algo que asegura que dentro de la empresa la información está protegida contra la divulgación a los usuarios no autorizados (confidencialidad), la modificación indebida (integridad) y el no acceso cuando sea necesario (disponibilidad). La seguridad de la información es un habilitador de negocios que está estrictamente ligada a la confianza de las partes interesadas, ya sea gestionando los riesgos del negocio o mediante la creación de valor para la empresa, como ventaja competitiva. En COBIT 5, los procesos *APO13 Manage Security, DSS04 Manage Continuity y DSS05 Manage Security Services* proveen una guía básica de cómo definir, operar y monitorear un sistema de gestión de seguridad general. [ISACA, 2012b]

- **Gestión de Riesgos**

Es un enfoque integral de manejo de riesgos o amenazas, que tiene como fin evaluar, administrar y comunicar estos riesgos, basados en los objetivos estratégicos de la organización. A continuación se describe algunas de las metodologías y/o métodos de Gestión de Riesgos.

- **OCTAVE**

OCTAVE es una metodología de gestión de riesgos que mejora el proceso de decisiones relativas a la protección y gestión de los recursos en una empresa de decisión. Fue desarrollado en el año 2001 por la Universidad Carnegie Mellon. La evaluación de riesgos se basa en tres principios básicos de la administración de la seguridad: confidencialidad, integridad, disponibilidad, mediante simple clasificación de la información crítica.

La metodología OCTAVE diseña un enfoque que permite conocer los problemas de seguridad y mejorar la postura de seguridad de su organización sin depender necesariamente de expertos y proveedores. Una evaluación con esta metodología proporciona una dirección para las actividades de seguridad de la información de una organización. [PYKA, 2006]

Figura 8. La división de los procesos y subprocesos de OCTAVE
Fuente: PYKA, 2006

- **MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)**

Se trata de una guía que se dirige a los directivos de la organización. Cuenta con 5 grandes categorías de activos:

- Entorno o soporte del sistema de información que comprende activos tangibles, equipamiento de suministro auxiliar y personal.
- Sistema de información que comprende hardware, redes propias, software de sistema y aplicaciones, etc.
- Información requerida, soportada o producida por el sistema de información que incluye datos informatizados, entrantes y resultantes, así como su estructuración y sus soportes.
- Funcionalidades que justifican al sistema de información.
- Otros activos, como la imagen de la organización, el fondo de comercio, entre otros.

Además el proceso MAGERIT consta de tres etapas principales, cada una de ellas contiene diversas actividades: [MAGERIT, 2012a]

- Planificación del análisis y gestión de riesgos, en el que se establecen las consideraciones necesarias para iniciar el proyecto.
- Análisis de Riesgos, en el que se identifican, valoran y estiman los diversos elementos del riesgo.
- Gestión de riesgos, se identifican los mitigantes de riesgos y se seleccionan los aceptables.

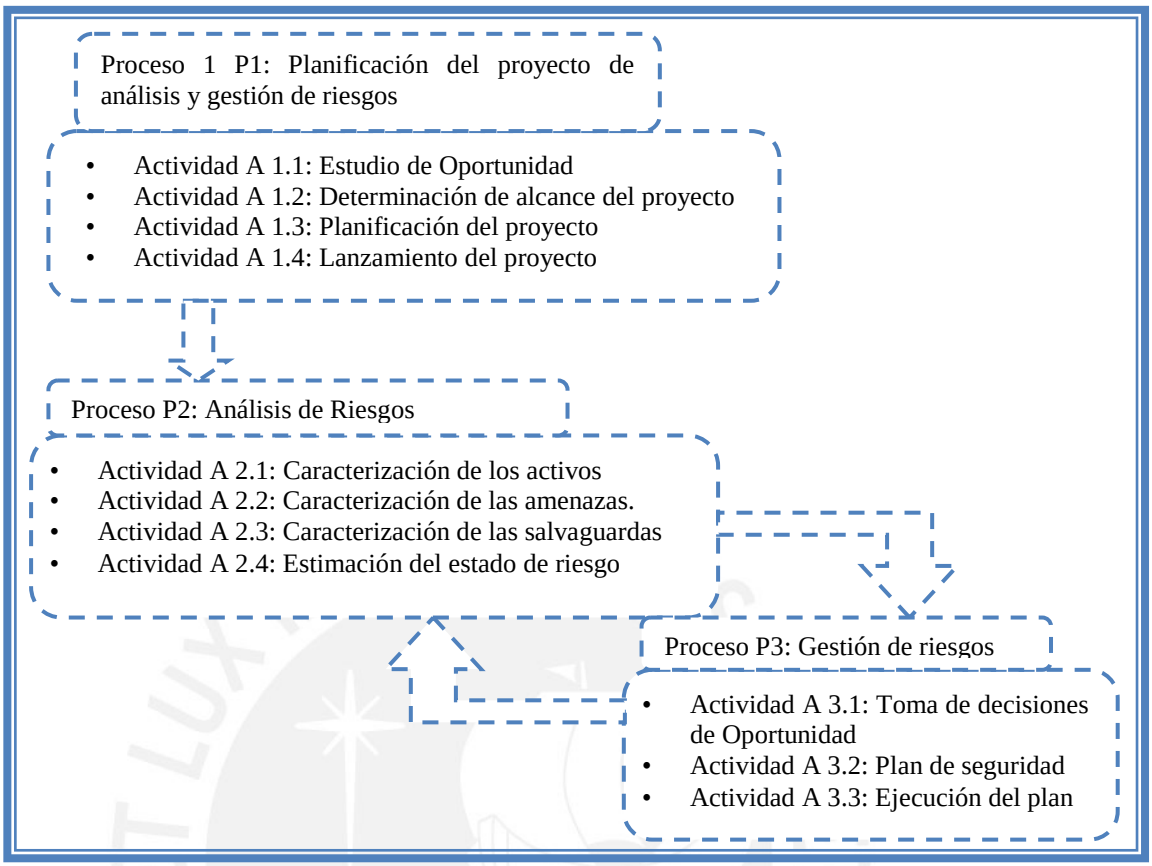


Figura 9. Esquema de procesos de MAGERIT
Fuente: MAGERIT, 2012b

- **ISO 31000:2009**

Según la norma ISO 31000:2009, una gestión eficaz del riesgo implica establecer una serie de principios y directrices, además debe estar estructurado con tres elementos clave: [ISO 31000, 2009]

- Los principios para la gestión del riesgo
- La estructura del soporte
- El proceso de gestión de riesgos

Mediante la aplicación de la norma ISO 31000, las organizaciones pueden comparar sus prácticas de gestión de riesgo con un punto de referencia reconocido internacionalmente, de igual manera la norma recomienda que las organizaciones desarrollen, apliquen y mejoren continuamente un marco de Gestión del riesgo como un componente integral de su sistema de gestión.

La guía ISO 73:2009, el vocabulario de Gestión de Riesgos, complementa la ISO 31000 y proporciona una colección de términos y definiciones relativas a la gestión de Riesgos. Ambas pueden aplicarse a cualquier entidad pública, privada, asociación, grupo o individuo.

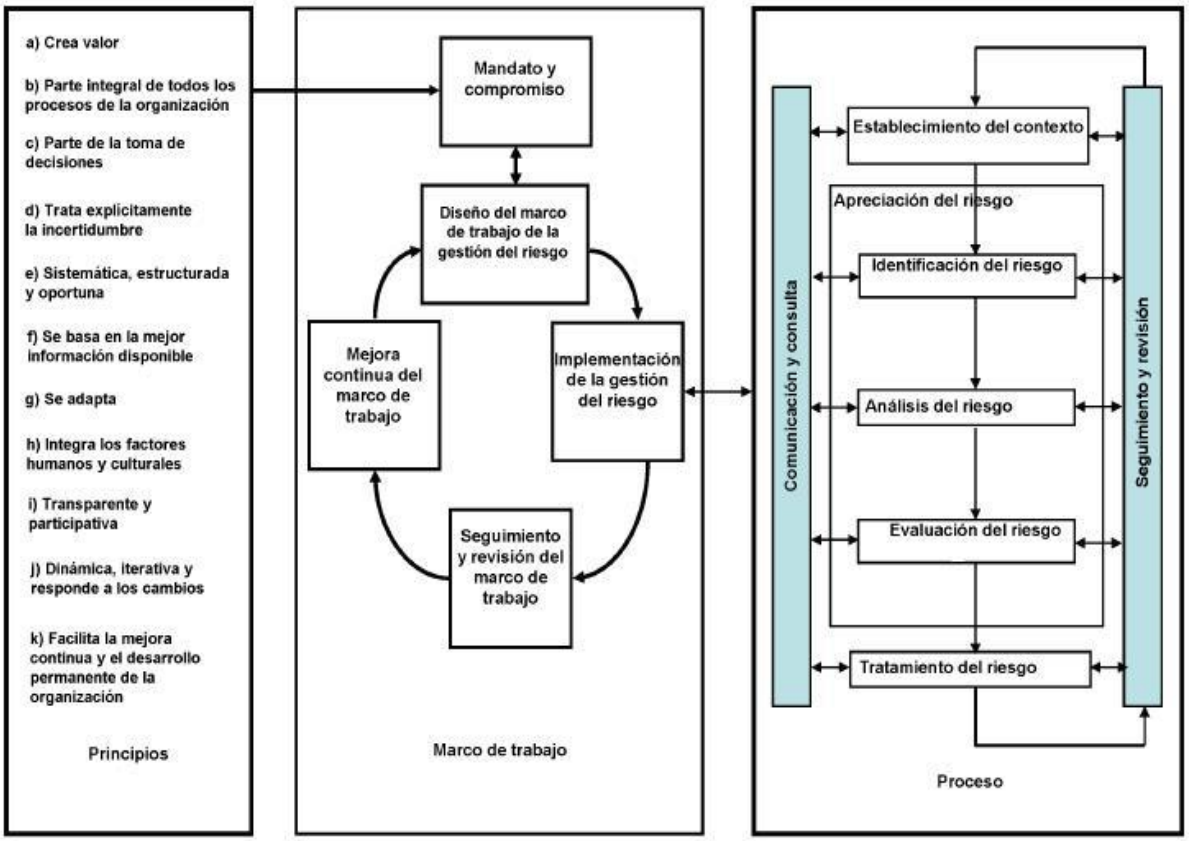


Figura 10. Framework para la Gestión de Riesgos de la ISO 31000:2009
Fuente: iso27000.es

- **RISK IT (Riesgos de Tecnología de Información)**

Risk IT Framework describe a detalle el modelo de procesos para la Gestión de Riesgos relacionados a las Tecnologías de información. En este modelo, las referencias están hechas al análisis de riesgos, análisis de escenarios, responsabilidades, indicadores clave de riesgos y otros términos relacionados a los riesgos. Además, contiene una guía práctica de Riesgos de TI, que especifica cómo lograr algunas de las actividades claves descritas en el modelo.

2 Estado del arte

En este apartado se describirá las formas y/o productos existentes de resolver el problema antes descrito.

2.1 Formas exactas de resolver el problema

Con respecto a la resolución del problema de inseguridad de información, se tiene que no se han encontrado formas exactas de resolverlo, pues esto depende del contexto y el rubro en el que la empresa se desempeñe, además una organización siempre estará expuesta a los diversos factores de riesgo que altere sus procesos de negocio.

2.2 Formas aproximadas de resolver el problema

Algunas formas aproximadas de resolver el problema, se enfocan en seguir algunas recomendaciones y establecer ciertas políticas de seguridad. Según una encuesta realizada a 250 organizaciones en 14 países de Latinoamérica realizado por Symantec, se muestra un fuerte incremento e interés en temas de seguridad, mientras los negocios presentan muchas variedades de riesgos como ciberataques, terrorismo, delitos tradicionales, desastres naturales, entre otros. Además se tiene que las amenazas han evolucionado en el tiempo, como los hackers, intrusos y ataques dirigidos. Esto ha generado pérdidas excesivas en las empresas. [SYMANTEC, 2011]

En base al reporte de seguridad, algunas recomendaciones de Symantec son:

- Desarrollar políticas de seguridad y reforzarlas con automatización incorporada y flujos de trabajo.
- Identificar y proteger información confidencial.
- Validar y proteger a todos los usuarios, sitios y dispositivos. Además autenticar las transacciones cuando sea apropiado.
- Manejar sistemas, implementando ambientes de operación segura, automatizar procesos y monitorear el estatus del sistema.
- Proteger la infraestructura, asegurando endpoints, mensajería y ambientes web.

Otra forma de resolver el problema es establecer en la empresa un Sistema de Gestión de seguridad de Información (SGSI).

Hasta el momento, en el Perú, no ha habido proyectos de implementación de SGSI en empresas inmobiliarias. Pero si se ha implementado Sistemas de Gestión de seguridad en entidades financieras y empresas aseguradoras, puesto que su regulador lo exige, en este caso la Superintendencia de Banca y seguros (SBS).

Otros casos como empresas de servicios de telefonía, se encuentra Telefónica del Perú, el cual cuenta con un SGSI, el cual en base a la norma internacional ISO 27001:2005, logró una certificación, para su Data Center, que brinda servicios de Outsourcing de TI, Disaster Recovery/Businnes Continuity, Hosting, Housing a las empresas de mayor envergadura en el país, y para sus centros de gestión de móviles, de banda ancha y de redes empresariales, que han sido elevados a estándares de clase mundial. [GESTION, 2013]
A nivel nacional, este caso se repite para otras 6 empresas más, como GMD, Hermes Transportes Blindados S.A, Hochschild Minning PLC, Oficina de Normalización Previsional (ONP), Telefónica Empresas, Telefónica de Gestión de servicios compartidos S.A.C.

A nivel internacional, Japón es el país con más certificaciones ISO 27001, cuenta con aproximadamente 4150 certificaciones. [IRIC, 2013]

Con respecto a la implantación de un SGSI, se encontró que una empresa inmobiliaria japonesa " Daiwa Real Estate Appraisal" implementó un Sistema de Gestión de Seguridad de Información con el fin de mejorar la satisfacción del cliente y establecer una base sólida para la empresa. Además, en el año 2009 adquirió la certificación ISO 27001 para establecer un sistema para la protección de información de sus activos.

Otros países, como España, cuentan con una asociación para el fomento de la seguridad de información, el cuál actúa en beneficio de la comunidad española y las empresas u organizaciones públicas y privadas; además promueve el conocimiento e implementación de los Sistemas de Gestión de la Seguridad de la Información en todo el mundo, de acuerdo con la familia de estándares ISO 27000. [ISMS, 2013]

2.3 Productos comerciales para resolver el problema

Existen productos comerciales específicos para el control técnico de un sistema de Gestión de seguridad de Información de una empresa, como los siguientes:

- Symantec Backup Exec 2012, es un producto integrado que protege entornos virtuales y físicos, simplifica copias de seguridad y recuperación después de un desastre. Además cuenta con una consola de administración de operaciones de gestión de copias de seguridad y recuperación de la infraestructura física y virtual. [SYMANTEC, 2012] Dentro de los beneficios clave que brinda están:

- Copias de seguridad físicas y virtuales unificadas
- Simple de gestionar y monitorizar
- Servicio de soporte

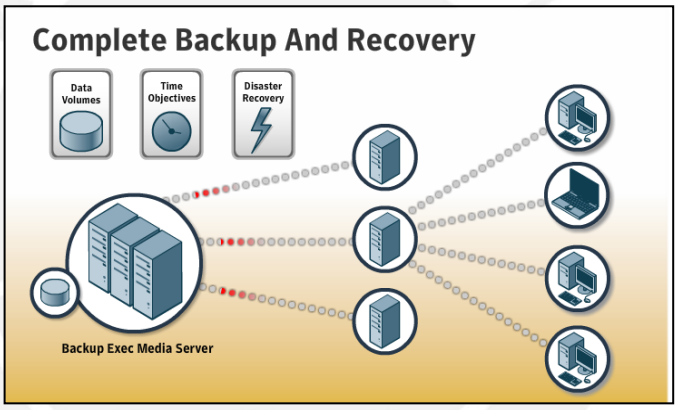


Figura 11. Características del producto Backup Exec 2012 de Symantec
Fuente: SYMANTEC, 2012

- Lookwise, se trata de un producto de S21sec, es una plataforma que da respuesta a las necesidades de la organización en materia de gestión de seguridad y cumplimiento normativo. Algunas de sus características son:

- Uniforme, centraliza la información de TI que se requiera.
- Sencillo, interfaz gráfica e intuitiva.
- Flexible y escalable, presenta una arquitectura modular que puede adaptarse a las exigencias. Admite arquitecturas en la nube, centralizadas y distribuidas.
- Integrado y de Alto rendimiento

- Correlación múltiple, establece conexiones necesarias entre diferentes dispositivos, sistemas o aplicaciones.

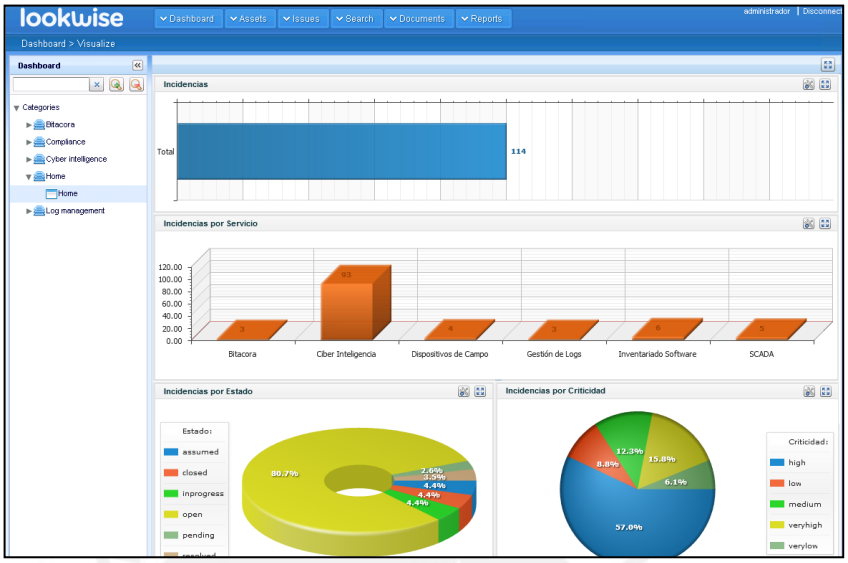


Figura 12. Vista del Cuadro de Mando del sistema Lookwise
Fuente: SYMANTEC, 2012

Otras compañías que ofrecen capacidades de seguridad como servicio, presentan los siguientes productos:

- CA CloudMinder de CA Technologies, proporciona un conjunto de capacidades de identity and access management (IAM) como servicios de nube alojados. La infraestructura del servicio de CloudMinder se encuentra alojada y monitoreada por CA.

- QualysGuard de Qualys, se trata de un sistema de administración de activos, cumplimiento de políticas y administración de vulnerabilidades en demanda.

- Symantec O3 Cloud Identity and Access Control de Symantec, es una plataforma de nube que proporciona control de acceso, seguridad de la información y administración de la información. El servicio permite sign on único en cualquier aplicación web.

- Symplified proporciona servicios de sign-on único federado, administración de identidad y de acceso.

2.4 Conclusiones sobre el estado del arte

Luego de presentar el estado del arte, se concluye que existen productos (programas, sistema, plataformas, entre otros) que resuelven de manera técnica algunos incidentes o necesidades específicas de seguridad de información. Si se desea que la organización controle, monitoree y sobretodo se proteja y preserve su información de manera centralizada y sistemática, es necesario adoptar un modelo o esquema de gestión de Seguridad de la Información, el cual va más allá de la Seguridad Informática, esto es porque involucra los procesos, personas y la Tecnología de Información. Para este caso, se ha decidido por establecer el diseño de un Sistema de Gestión de Seguridad de información (SGSI) en base a la norma internacional ISO/IEC 27001:2013, más adelante se explica la razón por las que se escoge un SGSI en la inmobiliaria de referencia.

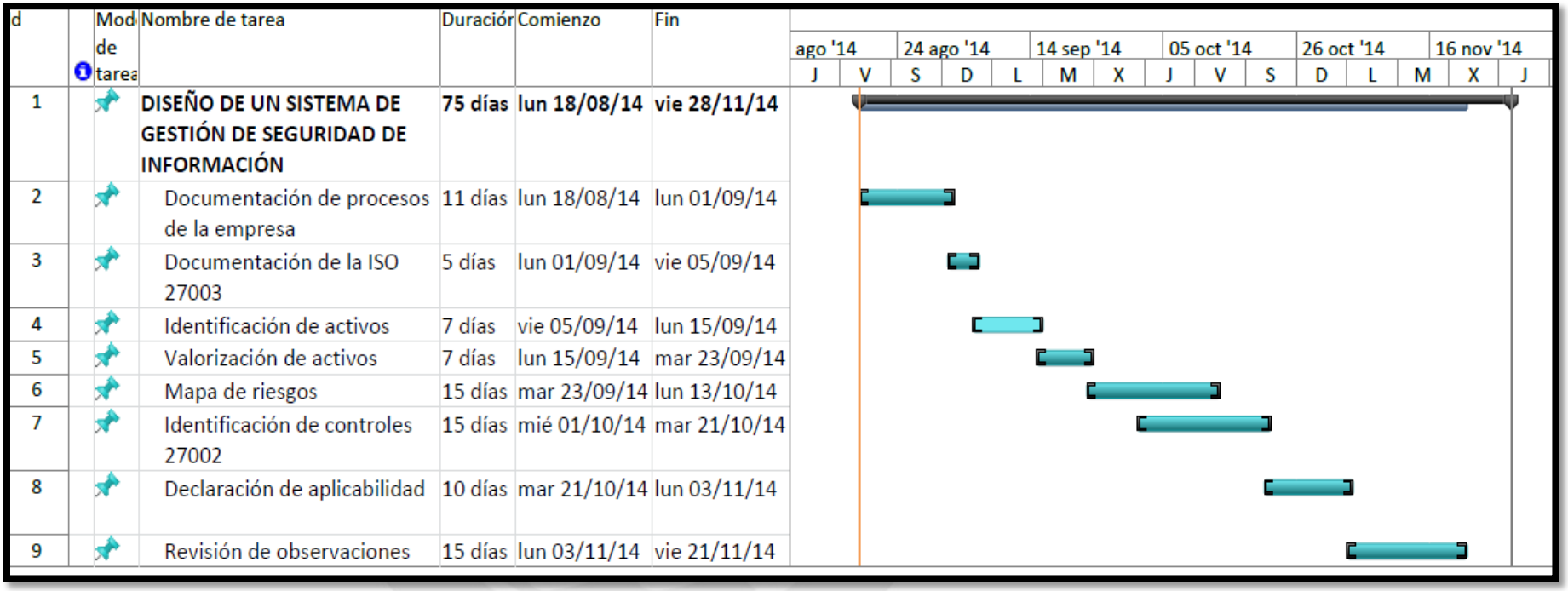
El desarrollo de la propuesta de solución servirá de guía para empresas del sector inmobiliario que deseen implantar un SGSI, la cual ofrece una visión global sobre el estado de sus sistemas de información, las medidas de seguridad que se están aplicando y los resultados que se están obteniendo de dicha aplicación, además ayudará a la organización a alcanzar un nivel más alto de madurez. Se pretenderá tener un enfoque alineado al negocio, de manera que implique la participación de los procesos, las personas y la tecnología.

Se tratará de un sistema activo e integrado en la organización, orientado a los objetivos empresariales y con proyección al futuro. También, cabe decir que cada vez que se incorpora una nueva herramienta o negocio de TI a la empresa se debe actualizar el análisis de riesgos, para poder mitigarlos de manera responsable con medidas de control adecuadas.

En nuestro país, pese a que las amenazas en seguridad como hackers, ataques cibernéticos, entre otros aumentan día a día y de hecho hacen más vulnerable a las empresas de diversos rubros; son muy pocas las que invierten en la gestión de seguridad de información. Es por eso, que el presente proyecto de tesis pretenderá concientizar a las compañías a poner énfasis en tomar las medidas necesarias para asegurar su propia información mediante el SGSI. Y dado que se trata de un sistema abierto se podrá incorporar tecnología nueva y éste se podrá adaptar a los cambios que pueda surgir.

3 Plan de Proyecto

3.1 Plan de actividades



d	Mod de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		**DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN**	**75 días**	**lun 18/08/14**	**vie 28/11/14**
2		Documentación de procesos de la empresa	11 días	lun 18/08/14	lun 01/09/14
3		Documentación de la ISO 27003	5 días	lun 01/09/14	vie 05/09/14
4		Identificación de activos	7 días	vie 05/09/14	lun 15/09/14
5		Valorización de activos	7 días	lun 15/09/14	mar 23/09/14
6		Mapa de riesgos	15 días	mar 23/09/14	lun 13/10/14
7		Identificación de controles 27002	15 días	mié 01/10/14	mar 21/10/14
8		Declaración de aplicabilidad	10 días	mar 21/10/14	lun 03/11/14
9		Revisión de observaciones	15 días	lun 03/11/14	vie 21/11/14

El siguiente plan de actividades muestra las tareas a realizar para el desarrollo del Diseño de Sistema de Gestión de Seguridad de Información para una empresa del sector inmobiliario. Asimismo, se considerará la revisión de documentos, normas y estándares, la recopilación de información, el trabajo de campo, la capacitación en herramientas útiles para el modelado de procesos, así como la definición de metodologías para realizar y analizar los riesgos de la empresa. Finalmente, se identificarán los controles asociados a los riesgos y se elaborará un documento de aplicabilidad que permitirá identificar cuáles de los controles, se aplican a las necesidades de la inmobiliaria.

3.2 EDT del proyecto

Para el presente proyecto se tienen los siguientes entregables, los cuales se describirán a partir del capítulo 3 y se detallarán en los anexos.

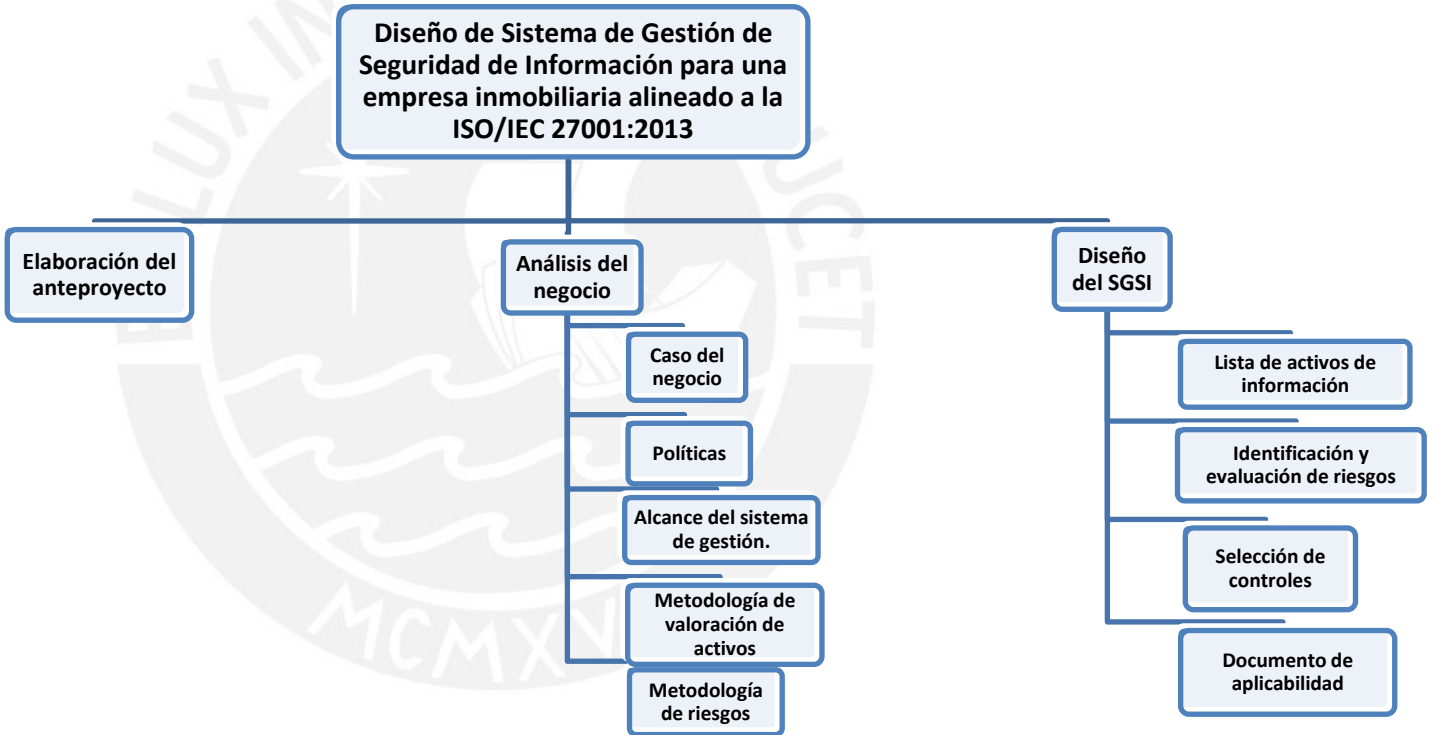


Figura 13. EDT del proyecto

CAPÍTULO 3

Este capítulo corresponde al primer resultado esperado del proyecto, acerca de la documentación requerida por la ISO/IEC 27001, el cual consiste en realizar un análisis del caso de negocio, el alcance con enfoque en procesos, descripción de la metodología de valorización de activos y finalmente la metodología de riesgos.

1 Caso de negocio

A continuación se presenta el caso de negocio de una organización privada del sector inmobiliario cuya principal actividad se enfoca en la unidad de negocio de vivienda.

1.1 Contexto estratégico

1.1.1 Visión general de la organización

La empresa del sector inmobiliario, de la cual se hace referencia, tienen como visión y misión:

Visión:
Ser líder en negocios de inversión, de promoción, desarrollo inmobiliario, habilitaciones urbanas, entre otras divisiones de negocio; de esta manera buscan generar valor para sus accionistas, clientes, colaboradores y la sociedad.

Misión:
Desarrollar negocios inmobiliarios, de estacionamientos, hoteleros y afines, creando espacios innovadores para vivir mejor, sustentados en el conocimiento de nuestros clientes, el compromiso y creatividad de nuestros colaboradores y el desarrollo sostenible de nuestro entorno.

Actividades principales:
La organización se dedica a toda clase de inversiones y negocios de promoción y desarrollo inmobiliario, habilitación urbana, administración de centros comerciales,

así como la prestación de servicios turísticos, hoteleros y de hospedaje. En el rubro de inversión figuran los servicios de administración, promoción, desarrollo y operación de playas de estacionamiento; sistema de peaje y actividades conexas.

En este caso, la unidad de negocio vivienda tiene una gran importancia, ya que representa un gran porcentaje de los ingresos de la inmobiliaria, es la unidad que genera más valor y en los últimos años ha tenido un continuo crecimiento.

Los productos inmobiliarios que se desarrollan son los siguientes:

* Habilitación urbana; se desarrollan terrenos para venta de lotes con instalaciones de servicios básicos (agua, desagüe, electricidad). La característica principal de este producto es el financiamiento directo (cuota inicial y el saldo financiado en letras). Dirigido principalmente a los niveles socioeconómicos C y D.

* Habilitación para vivienda secundaria; se desarrollan terrenos principalmente para venta de lotes para Casas de campo y Casas de playa.
* Vivienda unifamiliar; estos proyectos se realizan dentro del programa de Vivienda de Interés Social, Techo Propio y MiVivienda, y están dirigidos a niveles socioeconómicos D, de bajos recursos.

* Vivienda multifamiliar; se desarrollan proyectos del programa gubernamental MiVivienda, en zonas consolidadas de la ciudad de Lima, están orientados a los niveles socioeconómicos B y C.

1.1.2 Necesidades del negocio

Actualmente, en el Perú, el mercado inmobiliario ha ido creciendo sobretodo con nuevos proyectos de vivienda y oficinas; a pesar de ello los problemas no son ajenos a este sector, es el caso del proceso de adquisición de terrenos, la búsqueda de nuevos espacios, se ha convertido en uno de los principales problemas para constructoras e inmobiliarias, además de la burocracia para la aprobación de proyectos, así como la carencia o desactualización de planes urbanos.

Con respecto al marco regulatorio, se presenta la necesidad de cumplir con la reciente Ley de Protección de Datos Personales a fin de evitar las sanciones

aplicadas por el regulador, de manera que se puedan proteger y salvaguardar la información de clientes e inversionistas, así como información de los proveedores y los trabajadores de la inmobiliaria.

1.2 Análisis y recomendaciones

Por lo general, las empresas de negocio inmobiliario obtienen ingresos y generan utilidades en cientos de millones de soles, por lo que cualquier proceso o procedimiento mal realizado o fallido se traduce en pérdida directa para la empresa. Por ello, es vital mantener un orden adecuado así como cumplir con buenas prácticas que permitan asegurar la información en cada uno de los procesos involucrados. Justamente dentro de la empresa inmobiliaria, de la cual se hace referencia, se ha detectado la ausencia de procesos debidamente documentado o documentación desactualizada, esto hace que la organización no pueda controlar y medir de forma regular las características clave de sus operaciones y actividades que puedan tener un impacto significativo en el negocio.

Por otro lado, se tiene que históricamente, el sector inmobiliario, no ha sido sufrido ataques de seguridad de información de manera tan agresiva como otros sectores, como el de retail*, servicios financieros y el sector salud. Sin embargo, en la situación actual, se ha identificado que en la empresa inmobiliaria hay una mayor dependencia por las tecnologías de la información, asimismo el hecho de que las inmobiliarias creen, usen, almacenen y comparten cada vez más información que antes, ha hecho que las vulnerabilidades aumenten, y que las amenazas (como ataques de denegación de servicio, robo de información, desastres naturales, acceso no autorizado a sistemas de información, entre otros.) puedan aprovecharse de ellas.

Por ello, es necesario seguir un modelo de seguridad de información que permita adecuarse a la inmobiliaria y se alineen a los objetivos del negocio. En este caso, se recomienda definir un Sistema de Gestión de Seguridad de Información (SGSI), el cual servirá como herramienta, de mejora continua, que la organización dispone para implementar las políticas y objetivos de la Seguridad de información.

Retail, se refiere al sector económico que engloba a las empresas especializadas en la comercialización masiva de productos o servicios uniformes a grandes cantidades de clientes.

Asimismo, al ser parte de un sistema total de gestión, permitirá a los altos directivos a tomar las decisiones más adecuadas con respecto a la seguridad de los activos de información de la organización.

2 Definición de la política de seguridad de información

Como ya se ha descrito, la norma exige que la Alta Dirección tome un rol importante dentro del SGSI, por lo que debe demostrar el apoyo y su compromiso a través de la publicación y mantenimiento de una política relacionada a la Seguridad de información dentro de la inmobiliaria. Esta debe formalizarse en un documento, debe ser clara y estar alineada con los objetivos del negocio.

En el Anexo A se puede apreciar una propuesta del documento de la política de seguridad para que pueda ser revisada y aprobada por la Alta Dirección.

3 Alcance del Sistema de Gestión de Seguridad de Información

Tal y como se describió en el alcance del proyecto, el SGSI se enfocará en los procesos de la unidad de negocio de Vivienda; enfocándose principalmente en los procesos críticos del negocio. En la *Figura 13* se presenta un esquema de los macro-procesos del negocio que serán modelados con la notación BPMN 2.0.

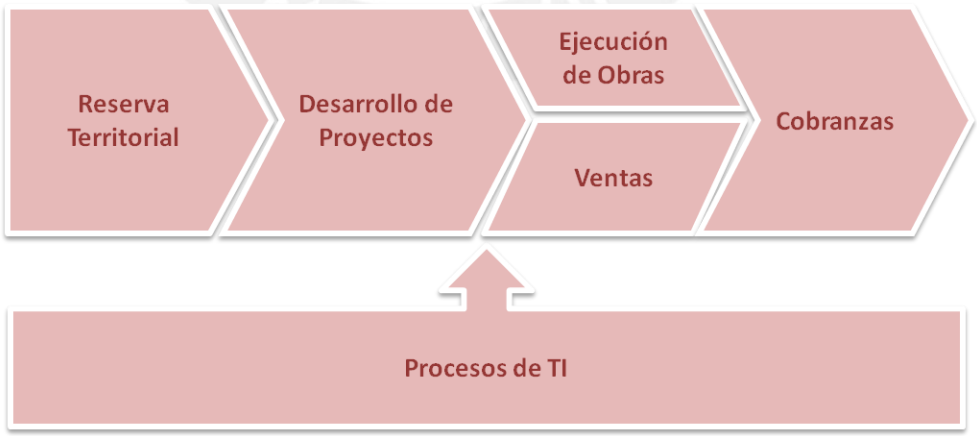


Figura 14. Macro-procesos de Vivienda

A continuación se describen los procesos del alcance, los cuales serán modelados con la notación BPMN 2.0:

3.1 Proceso de Reserva territorial

Este es el primer macro-proceso que inicia el ciclo del negocio de la Unidad de Vivienda, el proceso se divide en sub-procesos:

- Búsqueda de terrenos, el cual consiste en la búsqueda de nuevos terrenos identificados con posibilidad de compra.
- Negociación con el propietario,
- Estudio de factibilidad, y por último,
- Compra de terreno, cuyo objetivo es proveer de terrenos aptos para el desarrollo de proyectos inmobiliarios que permitan cumplir con las expectativas comerciales establecidas por el negocio.

En el Anexo B.1, se observa el mapa de proceso correspondiente al macro-proceso de Reserva Territorial.

3.2 Proceso de Desarrollo de proyectos

En este macro-proceso se encuentra:

* El proceso de Elaboración del Perfil Base del Proyecto, cuyo objetivo consiste en elaborar el expediente del perfil Base y flujo de caja para sustentar la viabilidad del proyecto.
* El proceso de Lanzamiento del proyecto, el cual establece los lineamientos y controles para el inicio y plan de un proyecto inmobiliario que inicia sus operaciones. Es el proceso por el cual se lanza al público la oferta de Lotes y viviendas para el inicio de Proyectos Inmobiliario.

En el Anexo B.2 se puede visualizar el mapa de los procesos mencionados.

3.3 Proceso de Ejecución de obras

Incluye los procesos:

* Revisión y aprobación de valorizaciones: su objetivo es realizar el seguimiento y control en la revisión y aprobación del avance de obra presentado por el contratista.
* Cierre de Obra: su objetivo es definir las actividades y lineamientos necesarios para culminar las obras del proyecto, y pasar de producto en proceso a producto terminado.

* Carga de Plano, cuyo objetivo es contar con la versión final de los planos de los proyectos ejecutados, considerando los criterios técnicos respectivos en los tiempos establecidos.

En el Anexo B.3 se puede observar los mapas respectivos a los procesos antes descritos.

3.4 Proceso de Ventas

Incluye los procesos:

* Prospección de clientes: Establecer las actividades requeridas para la venta de productos inmobiliarios a través del canal de venta de prospección, el cual se inicia con el envío de la Base de datos de clientes prospectos hasta la confirmación de la separación del inmueble.
* Venta de habilitaciones urbanas, cuyo objetivo es establecer las actividades requeridas para la venta de lotes en las plazas donde la entidad realiza operaciones. Se aplica desde la separación del inmueble hasta la firma de los contratos, una vez realizado los abonos.

En el Anexo B.4 se puede visualizar el mapa de estos procesos.

3.5 Proceso de Cobranzas

Dentro de este macro-proceso se modelará el proceso de Administración de Letras, cuyo objetivo es establecer las actividades requeridas para el control y seguimiento de letras por pagos generados en los procesos de ventas.

En el Anexo B.6, se observa el mapa de procesos correspondiente a Cobranzas.

Dentro de los procesos de Tecnologías de información se encuentra:

3.6 Proceso de Administración de cuentas de usuario

Se encuentran los subprocesos:

* Alta de cuenta de usuario, en el que se establecen lineamientos y controles para la distribución de activos y accesos de los distintos sistemas o aplicativos al colaborador.

* Modificación de acceso, y
* Baja de cuenta de usuario, consiste en normar los controles de baja de accesos de usuario para el aseguramiento del proceso de recuperación de credenciales.

3.7 Proceso de Administración de infraestructura

Se encuentran los subprocesos de Respaldo y restauración de información y Revisión periódica de niveles de acceso.

En el Anexo B.7, se puede visualizar el mapa de procesos correspondiente a Tecnología de información.

Finalmente, luego de definir los procesos del alcance del Sistema de Gestión de seguridad de información, se definirán las metodologías de valorización de activos y de gestión de riesgos a usar, que serán adaptadas a la situación de la empresa.

4 Metodología de valorización de activos

Se denomina activos a aquellos que otorgan valor a la organización y por tanto debe protegerse; para ello se describirá la metodología a usar en la valorización de activos.

Tal y como se establece en la norma ISO/IEC 27001, antes de gestionar los riesgos dentro de la organización, se identificará y se evaluará los activos de información (tangibles e intangibles) dentro cada proceso del alcance.

4.1 Identificación de activos

Los activos de información son archivos, bases de datos, contratos y acuerdos, documentación de los sistemas, manuales de usuario, material de capacitaciones, aplicaciones, software de sistema, equipos informáticos y de comunicaciones, servicios informáticos y de comunicaciones, y finalmente las personas, que son la última instancia, generan, transmiten y destruyen la información.
Para facilitar la valorización, se ha clasificado a los activos de la siguiente manera:

TIPO	DESCRIPCIÓN
Datos	Cualquier dato que se genere, recoja, gestione, transmite y destruyen en la organización.
Aplicaciones	Software de sistemas que se utiliza para la gestión de información.
Personal	Se encuentran tanto los empleados de la organización, como los clientes, usuarios, y todos aquellos que tengan acceso a los activos de información de la empresa.
Servicios	Se consideran los servicios internos, los que algún área de la organización suministra a otra; y los servicios externos, aquellos que la organización suministra a clientes y usuarios.
Tecnologías	Equipos para gestionar la información y comunicaciones.

Tabla 3. Clasificación de activos de información.

4.2 Inventario de activos

El inventario de activos que se usará tendrá como finalidad recoger los activos más importantes que se deben identificar de manera clara. Este inventario de activos es la base para la gestión de los mismos, ya que incluye toda la información necesaria para mantenerlos operativos e incluso puedan recuperarse ante un desastre.

Cada activo tendrá la siguiente información:

* Identificación del activo(ID): un código para ordenar y localizar los activos.
* Tipo de activo: se refiere a alguna categoría que pertenece el activo.
* Nombre: nombre del activo.
* Descripción: una breve descripción del activo para identificarlo sin ambigüedades.
* Propietario: es la persona responsable del activo.
* Ubicación: se especifica la ubicación del activo, puede ser físico y/o electrónico.

4.3 Valorización de activos

Una vez se haya identificado los activos, el siguiente paso a realizar es valorarlos, es decir, se estimará el valor que tienen para la organización y cuál es la importancia para la misma. Para calcular este valor, se considera la magnitud del daño que puede suponer para la organización que un activo resulte dañado en cuanto a su disponibilidad, integridad y confidencialidad.

En este caso se valorará una escala cuantitativa de acuerdo a los criterios de disponibilidad, integridad y confidencialidad, siendo el número 1 el de menor relevancia y el número 4 con el valor más relevante. En la siguiente tabla se muestra los criterios y sus respectivos valores.

Criterio	*Valor*	*Descripción*
Disponibilidad	**1**	El activo debe estar disponible por lo menos 25% del tiempo que se necesite. No existe riesgo operacional, reputacional, ni legal si el activo de información se ha eliminado o no está disponible.
	2	El activo debe estar disponible por lo menos 50% del tiempo que se necesite. Si no lo estuviera o si fuese destruido puede ocasionar daños leves en la organización, que afecten los intereses legales, operacionales y reputacionales.
	3	El activo debe estar disponible por lo menos el 75% del tiempo que se necesite. Si no lo estuviera o si fuese destruido ocasionará daños que serán perjudiciales en la organización, que afecten los intereses legales, operacionales y reputacionales.
	4	El activo debe estar disponible el 100% del tiempo que se necesite. Si no lo estuviera o si fuese destruido ocasionará daños catastróficos para la organización, afectarán los intereses legales, operacionales o reputacionales, y causarán pérdidas financieras.
Integridad	**1**	El activo debe estar correcto y completo por lo menos el 25% de las veces que se necesite. No existe pérdidas financieras ni riesgo operacional, reputacional, ni legal.
	2	El activo debe ser correcto y completo al menos el 50% de las veces que se necesita. Puede ocasionar daños leves en la organización, que afecten los intereses legales, operacionales y reputacionales.
	3	El activo debe ser correcto y completo al menos el 75% de las veces que se necesite; si no lo estuviera, puede ocasionar daños que serán perjudiciales para los intereses legales, reputacionales, operacionales y financieros de la organización.
	4	El activo debe ser correcto y completo el 100% de las veces utilizadas. De no cumplir con lo anterior, puede causar daños catastróficos para la organización, y afectará los intereses legales, operacionales o reputacionales, además de pérdidas financieras significativas.

Confidencialidad	**1**	El activo es publicada o de conocimiento del público en general, por lo tanto, no existe ningún riesgo legal, reputacional, operacional, ni financiero.
	2	El activo podrá ser divulgado hacia los colaboradores. Si se cumple con lo anterior no será perjudicial para los intereses legales, reputacional, operacional, ni financiero.
	3	El activo contiene información sensible, ya sea información personal, financiera, entre otros. Su divulgación puede ser perjudicial para los intereses legales, reputacional o financieros de la organización.
	4	El activo contiene información altamente sensible. Su divulgación puede causar daños catastróficos, afectando los intereses legales, reputacionales, y financieros.

Tabla 4. Criterios para valorización de activos.

Como resultado de la identificación de activos se obtiene un listado de los activos involucrados en el alcance del SGSI relacionados con un determinado proceso y con su respectiva valorización. El valor final del activo será el promedio de los tres valores en base a los criterios (disponibilidad, integridad y confidencialidad); en la Figura 15. se describe el valor cualitativo promedio del activo.

Valor promedio de activo	Descripción
4	Muy Alto, contiene información confidencial y en muchos casos la disponibilidad debe ser del 100%.
3	Alto, puede contener información confidencial, se debe cumplir con la integridad del activo.
2	Medio, no contiene información sensible, pero debe cumplir con algunos criterios como disponibilidad e integridad.
1	Bajo, los activos ubicados en este valor promedio, son activos de carácter público.

Figura 15. Valor promedio del activo de información.

El inventario de activos como se observa en el Anexo C.

5 Metodología de riesgos

A nivel general, la ISO 31000 establece que los principios de gestión de riesgos son los siguientes:

* Crear valor.
* Está integrada a los procesos de la organización.
* Forma parte de la toma decisiones.
* Trata explícitamente la incertidumbre.
* Es sistemática, estructurada y adecuada.
* Está basada en la mejor información disponible.
* Está hecha a medida.
* Tiene en cuenta factores humanos y culturales.
* Es transparente e inclusiva.
* Es dinámica, iterativa y sensible al cambio.
* Facilita la mejora continua de la organización.

Con esto se puede establecer en la organización un marco de riesgos que permitirá gestionar efectivamente sus riesgos. Para el presente proyecto, se adaptarán las actividades del proceso de Gestión de Riesgos al diseño del Sistema de seguridad de Información. En primer lugar, se establece el contexto externo e interno, el cual impacta en los objetivos de la inmobiliaria. Algunos aspectos externos más influyentes son:

* Leyes y normas regulatorias, entre estos tenemos la ley de protección de datos personales, la cual está vigente desde el año 2013 y a la fecha todas las empresas tanto públicas como privadas deben estar alineados a esta ley. Para el caso, de la empresa inmobiliaria, los datos a proteger son los de sus colaboradores, clientes, proveedores, y sobre todo de los inversionistas, quiénes se guían de la reputación y del valor que pueda generar un proyecto inmobiliario.

* Perspectivas económicas y del mercado objetivo del cliente, los clientes buscan productos inmobiliarios que les inspire confianza, se presente propuestas claras y tengan los mejores precios.

* Habilitación de terrenos en Lima y Provincias.
* Variación del dólar en los últimos meses

Siguiendo el marco de la metodología de gestión de riesgos, se debe identificar los riesgos de cada uno de los procesos del alcance de la unidad de negocio de Vivienda.

5.1 Identificación del riesgo

La identificación del riesgo se realiza determinando las causas, con base en los factores internos y/o externos analizados para la organización, que afecten el logro de los objetivos. Es importante centrarse en los riesgos más significativos que afectan a los objetivos de los procesos y a los institucionales, es aquí donde la alta dirección debe tomar un papel proactivo en el sentido de visualizar en el contexto estratégico los factores que pueden afectar el curso institucional.

Los conceptos que se usarán para identificar los riesgos son:

* Código Riesgo: Identificador del riesgo
* Proceso: Nombre del proceso.
* Subproceso.
* Riesgo: posibilidad de ocurrencia de que un evento no deseado pueda suceder.
* Causas: factores externos e internos y actúan como agentes generadores de riesgo.
* Descripción: características generales o formas en que se manifiesta el riesgo.
* Efectos: constituyen las consecuencias de la ocurrencia del riesgo.

5.2 Análisis del riesgo

Para analizar el riesgo se debe establecer la probabilidad de ocurrencia del mismo, así como sus consecuencias, esto finalmente orientará a la clasificación del riesgo. Esta fase depende de la información obtenida en la etapa de identificación. Existen dos aspectos principales que determinarán el análisis de riesgo:

* Probabilidad: posibilidad de ocurrencia del riesgo, la cual se puede medir con criterios de frecuencia.
* Impacto: consecuencias que pueden ocasionar la materialización del riesgo en la organización.

PROBABILIDAD	DESCRIPCIÓN
Frecuente	Evento que sucede con frecuencia o que posiblemente ocurra
Moderado	Evento que tiene cierta posibilidad de ocurrir.
Ocasional	Evento que ocurre sólo en ocasiones, usualmente depende de una segunda causa.
Remoto	Evento que no es probable que suceda.
Improbable	Evento que es improbable que suceda o tenga muy baja expectativa de ocurrencia

IMPACTO	DESCRIPCIÓN
Insignificante	El impacto ocasionado es muy bajo, los procesos no serán afectados con intensidad de manera que pueden continuar con el desarrollo del flujo con normalidad.
Menor	El impacto es bajo, los procesos son afectados de tal manera que se necesitará a lo más una hora para poder continuar con las actividades.
Medio	Este impacto tiene como consecuencia que se dedique horas para poder resolver el problema y así continuar con el flujo de los procesos.
Crítico	El impacto que ocasiona en los procesos es alto. Podría tomar días para resolver el problema.
Catastrófico	El impacto que ocasiona en los procesos es muy alto. Podría tomar días para resolver el problema.

Tabla 5. Categorías de probabilidad e impacto de riesgos.

En la *Figura 16,* se muestra la relación entre Probabilidad e Impacto, el cual permitirá medir el riesgo.

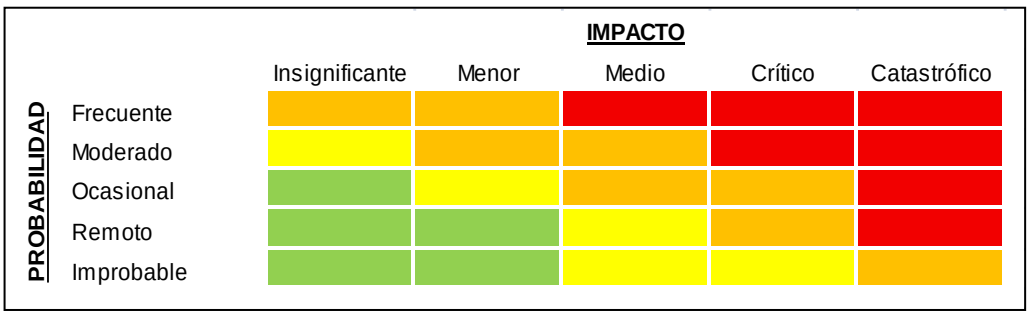


Figura 16. Matriz de calor para el análisis de riesgos.

5.3 Evaluación del riesgo

La evaluación involucra comparar niveles de riesgo con criterios definidos en el contexto. El objetivo de esta evaluación es la de identificar y evaluar los riesgos, los cuales son calculados por una combinación de valores de activos y niveles de requerimiento de seguridad. Con base en esta comparación, se puede considerar la necesidad de tratamiento; además las decisiones se deben tomar de acuerdo con los requisitos legales, reglamentarios y otros.

La evaluación de riesgos también puede tener como resultado la decisión de no tratar el riesgo de ninguna manera diferente de los controles existentes. A continuación, se presenta la matriz cualitativa que permitirá evaluar los riesgos identificados en la entidad inmobiliaria.

			IMPACTO		
PROBABILIDAD	Insignificante	Menor	Medio	Crítico	Catastrófico
Frecuente	**A**	**A**	**E**	**E**	**E**
Moderado	**M**	**A**	**A**	**E**	**E**
Ocasional	**I**	**M**	**A**	**A**	**E**
Remoto	**I**	**I**	**M**	**A**	**E**
Improbable	**I**	**I**	**M**	**M**	**A**

Convenciones
E = riesgo extremo
A = alto riesgo
M = riesgo moderado
I = riesgo inferior

Figura 17. Matriz cualitativa para la evaluación de riesgos.

Actualmente, en la organización no se encuentra establecido el apetito de riesgo, es decir, no se ha definido hasta qué nivel de riesgo podrían tomarlo como aceptable. Por lo que se propone lo siguiente:

Si bien la empresa a la que se hace referencia, pertenece a la calificación de Grandes empresas, el apetito de riesgo que la organización estaría dispuesta a aceptar serán las que se encuentren en las convenciones de riesgo inferior y riesgo moderado, lo que se encuentren en la convención de alto riesgo (A) en la matriz cualitativa deben ser monitoreados y controlados constantemente. Y finalmente, no se aceptará por ningún motivo los riesgos con la convención riesgo extremo, por lo que deberán ser controlados y monitoreados de inmediato.

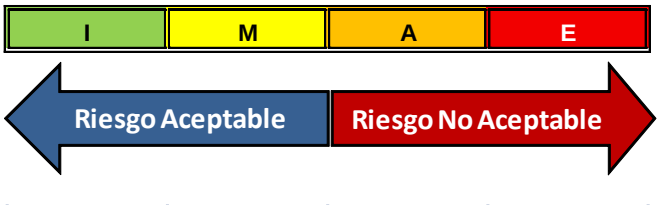


Figura 18. Apetito de riesgo para el tratamiento de riesgos.

En el Anexo D. se puede visualizar el mapa de riesgos en el que se identificaron y evaluaron los riesgos relacionados a cada proceso del alcance.

5.4 Tratamiento del riesgo

El tratamiento del riesgo se define como el conjunto de decisiones tomadas con cada activo de información.

Las decisiones para tratar el riesgo pueden incluir las siguientes opciones:

* **Evitar** el riesgo al decidir no iniciar o retirar la fuente de riesgo.
* **Aceptar** el riesgo cuando no es posible mitigarlo y se debe continuar la actividad que lo originó.
* **Reducir** el riesgo cuando se encuentra fuera del apetito de riesgo, se puede cambiar la probabilidad de ocurrencia o cambiar las consecuencias.
* **Transferir** el riesgo fuera del apetito de riesgo, el riesgo se comparte con una o varias partes, pueden ser agentes externos.

Finalmente se debe preparar planes de tratamiento del riesgo, esta información debe incluir:

- Las razones para la selección de las opciones de tratamiento, que incluyan los beneficios que se espera obtener.
- Los responsables de aprobar el plan y los responsables de implementarlo.
- Acciones propuestas.
- Requisitos de recursos, incluyendo contingencias.
- Requisitos de monitoreo y reporte.

Los planes de tratamiento se deben integrar con los procesos de gestión de la organización y discutir con las partes involucradas pertinentes. En el siguiente capítulo se identificarán los controles necesarios para cada riesgo identificado fuera del apetito de riesgo.

CAPÍTULO 4

Este capítulo corresponde a la identificación de los controles de Seguridad de Información en base al mapa de riesgos realizado en el capítulo anterior.

1 Identificación de controles según la ISO/IEC 27002:2013

La selección de controles depende de las decisiones de la organización basada en los criterios de aceptación de riesgos, las opciones de tratamiento de riesgo y el enfoque general de gestión de riesgos aplicado a la organización; también debe estar sujeta a las leyes y regulaciones nacionales e internacionales pertinentes. [ISO 27002, 2013]

Por ello, luego de evaluar los riesgos, sólo se tomarán aquellos riesgos que se encuentren fuera del apetito, es decir, aquellos que se consideran como riesgo No Aceptable, a los cuales se les asignará uno o más controles para su tratamiento. Todo esto constituye el Plan de Tratamiento de Riesgos.

A continuación se presenta una breve explicación de cada uno de las cláusulas de controles que según la ISO 27002:2013 se pueden implementar dentro de cualquier organización. Algunos de los controles en esta norma serán considerados como principios para la gestión de seguridad de la información y se aplicarán a los riesgos identificados en la inmobiliaria:

Cláusulas de los controles ISO/IEC 27002:2013	Descripción de objetivo
5. POLÍTICAS DE SEGURIDAD.	Proporcionar la gestión para la dirección y apoyo a la seguridad de información de acuerdo con los requerimientos del negocio, las leyes y regulaciones pertinentes.
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de información dentro de la organización. Garantizar la seguridad de teletrabajo y el uso de dispositivos móviles.

7. SEGURIDAD EN LOS RECURSOS HUMANOS.	Asegurar que los empleados y contratistas entiendan sus responsabilidades de acuerdo a los roles que poseen. Asimismo, deben conocer y cumplir sus responsabilidades de seguridad de información. Finalmente, se debe proteger los intereses de la organización como parte del proceso del cambio o terminación del empleo.
8. GESTIÓN DE ACTIVOS.	Identificar los activos de la organización y definir apropiadamente las responsabilidades de protección. Garantizar que la información recibe un nivel adecuado de protección de acuerdo a su importancia en la organización. Finalmente, evitar la divulgación no autorizada, modificación, eliminación de la información almacenada en los medios de comunicación.
9. CONTROL DE ACCESOS.	En primer lugar, se debe limitar el acceso a la información y a las instalaciones de procesamiento de información. Garantizar el acceso de usuarios autorizados y evitar y prevenir el acceso no autorizado a los sistemas y servicios. Hacer a los usuarios responsables de proteger su información de autenticación.
10. CRIPTOGRAFÍA.	Garantizar el uso adecuado y eficaz del cifrado para proteger la confidencialidad, autenticidad y/o integridad de la información.
11. SEGURIDAD FÍSICA Y DEL ENTORNO.	Prevenir el acceso físico no autorizado, daños e interferencia a la información de la organización y a las instalaciones de procesamiento de información. Así como, evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las operaciones de la organización.
12. SEGURIDAD EN LAS OPERACIONES.	Asegurar que las operaciones sean correctas y seguras en las instalaciones de procesamiento de información. Asegurar que estas instalaciones y la información estén protegidas contra el malware. Evitar la pérdida de datos. Registrar eventos y generar evidencia. Garantizar la integridad de los sistemas operativos. Evitar la explotación de vulnerabilidades técnicas. Y minimizar el impacto de las actividades auditadas en los sistemas operativos.
13. SEGURIDAD EN LAS COMUNICACIONES.	Garantizar la protección de la información en las redes y las instalaciones de procesamiento de información. Mantener la seguridad de la información transferida desde la organización con cualquier entidad externa.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS.	Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas. Finalmente, garantizar la protección de los datos utilizados para pruebas.

15. RELACIONES CON PROVEEDORES.	Garantizar la protección de los activos de la organización que sea accesible por los proveedores. Mantener un nivel de seguridad de la información y de prestación de servicios alineado con los acuerdos con los proveedores.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluidos los de comunicación de los eventos de seguridad y los puntos débiles.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	La continuidad de la seguridad de Información se incluirá dentro de los sistemas de gestión de continuidad de negocio de la organización. Garantizar la disponibilidad de instalaciones de procesamiento de información.
18. CUMPLIMIENTO.	Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas a la seguridad de la información y a los requisitos de seguridad. Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.

Tabla 6. Cláusulas de controles de la norma ISO/IEC 27002:2013.

En el Anexo E. se puede visualizar el Plan de Tratamiento de los Riesgos identificados, así como los controles y las cláusulas asociadas.

2 Declaración de aplicabilidad

Luego de identificar los controles para todos los riesgos con nivel No Aceptable para la organización, se detallarán cuáles se aplican o no en el contexto de la empresa inmobiliaria. El documento en el que se especifican los controles que aplican dentro del Sistema de Gestión, se denomina Declaración de Aplicabilidad o SoA[*].

En el Anexo F. se presenta una tabla con la declaración de aplicabilidad.

SoA, Statement of Applicability, es un documento que lista los objetivos y controles que se van a implementar en una organización, así como las justificaciones de aquellos controles que no serán implementados. [ISO 27001, 2013]

CAPÍTULO 5

En el siguiente capítulo se presentan las observaciones, conclusiones y recomendaciones del proyecto de Diseño de un Sistema de Gestión de Seguridad de Información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013.

1 Observaciones

En los últimos años, la seguridad de información no se percibía como una prioridad dentro de la inmobiliaria, pues no lo consideran parte de su giro de negocio; sin embargo, luego de la publicación y aprobación de la ley de Protección de Datos personales, se ha puesto énfasis a la seguridad de información de clientes, proveedores e inversionistas, así como de colaboradores de la empresa. Asimismo, al darse cuenta de la relevancia de la información que se maneja en sus procesos críticos de negocio, tienen la necesidad de proteger información de sus proyectos inmobiliarios, tales como el informe de zonas de terreno, los perfiles de proyecto y expedientes técnicos y comercial del proyecto.

Con respecto al entorno de seguridad de información dentro de la inmobiliaria, se observó que no hay una política de seguridad de información que se alinee a los objetivos organizacionales, y que según la ISO/IEC 27002: 2013, proporciona a la Alta dirección los lineamientos para llevar a cabo una adecuada gestión de la seguridad de información de acuerdo con los requerimientos del negocio, las leyes y regulaciones pertinentes.

Con respecto al análisis de riesgos de seguridad identificados en la organización, se observa que al menos más del 50% cae dentro del nivel de Alto Riesgo, es decir fuera del riesgo Aceptable para la empresa; y que al menos un 40% se considera como riesgo de nivel Moderado, este nivel de riesgo está dentro del apetito de la organización inmobiliaria. En la *Figura 19*. se observa lo descrito anteriormente.

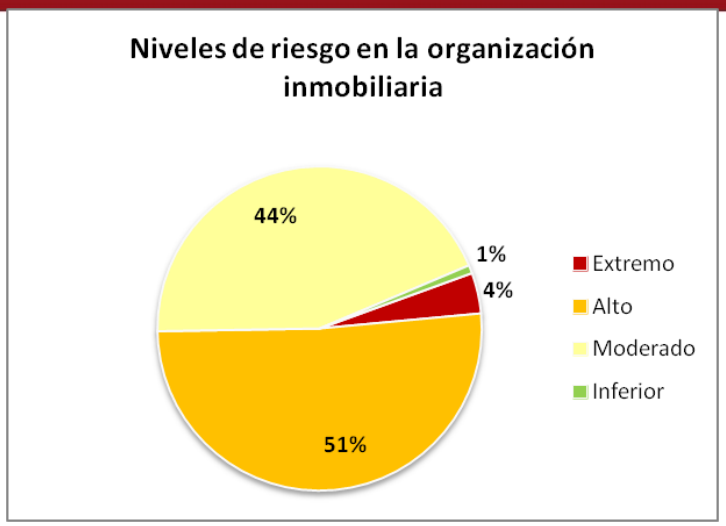


Figura 19.Niveles de riesgo en la organización inmobiliaria.

2 Conclusiones

A partir del desarrollo del proyecto se concluye lo siguiente:

En primer lugar, la Alta dirección tiene un papel muy importante en el Sistema de Gestión de Seguridad de Información, pues además de tomar las decisiones estratégicas más importantes de la organización, su compromiso será fundamental para llevar a cabo el SGSI e imprescindible para la implementación de los controles.

Es necesario establecer una Política de Seguridad de Información que contenga los lineamientos para una eficiente administración de la información con el fin de garantizar la seguridad de los sistemas que satisfaga el requerimiento del negocio y de mantener la integridad de la información, de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad.
Asimismo, la Alta Dirección debe difundir esta política, conocer y dar a conocer a todo el personal que labora en la empresa, de igual manera, el personal es responsable de conocer y cumplir con lo que se especifica.

En vista de las amenazas, tanto externas como internas, a las que se ve expuesta la inmobiliaria, es necesario establecer roles y responsabilidades dentro de la organización relacionados a Seguridad de Información, para garantizar el cumplimiento de las políticas de seguridad de Información, así como el monitoreo y seguimiento de los riesgos de información.

Actualmente, de acuerdo al análisis de riesgos, el status de la seguridad en la inmobiliaria se encuentra a un nivel bajo, esto es porque hay una gran cantidad de riesgos que se consideran como No aceptables y no tienen controles asociados para mitigarlos es decir se están aceptando riesgos que posiblemente se materialicen en cualquier momento y esto genere pérdidas directas al negocio.

Finalmente, al no contar con una regulación específica que exija tomar un modelo de Seguridad de información en la inmobiliaria, ésta deberá trabajar especialmente en el aspecto de cultura de seguridad a todo nivel, pues es necesario concientizar a todo el personal para llevar a cabo el SGSI.

3 Recomendaciones y trabajos futuros

Para lograr una efectiva implementación del Sistema de Gestión de Seguridad de Información en la inmobiliaria, se recomienda seguir con los siguientes factores de éxito; en primer lugar tener el apoyo constante de la Alta dirección, segundo, seguir con el diseño del SGSI, el cual se desarrolló a lo largo del proyecto; y tercero, generar conciencia en la organización. Este último aspecto no siempre se logra de inmediato, pues muchas personas se muestran reacias al cambio, lo que puede ocasionar inconvenientes en la implementación del SGSI.

Por ello, con el objetivo de generar una cultura de seguridad dentro de la organización, es decir concientizar a cada colaborador de la importancia de sus actividades de seguridad de información y la manera de cómo contribuye a los objetivos del SGSI, se recomienda realizar capacitaciones permanentes a todo el personal de la empresa.

Además, se recomienda crear el rol de Oficial de Seguridad de información, conocido como CISO por sus siglas en inglés (Chief Information Security Officer), quien será el encargado de planificar, presupuestar y verificar el rendimiento de los componentes de la seguridad de la información; así como de realizar una correcta gestión de riesgos para la toma de decisiones.

También se puede incluir el uso de plataformas tecnológicas o aplicaciones con la automatización del SGSI que puede ayudar a la Alta dirección de la inmobiliaria a cumplir con su compromiso y a llevar a cabo una revisión exhaustiva.

Si bien la Alta Dirección se encarga de revisar el SGSI, es necesario llevar una revisión periódica, a través de auditorías, esto es para detectar brechas de seguridad referidas en la Norma ISO/IEC 27001 y para establecer mejoras en el sistema. Por ello, se recomienda que el auditor del sistema no debe haber participado en la implementación del mismo, con una medida para mantener la objetividad y la independencia entre ambos procesos.

Y por último, se debe tener en cuenta que la seguridad total no existe, es por ello que se debe incurrir en un mantenimiento constante del SGSI que implica que la organización deba realizar cuando crea conveniente las mejoras identificadas, para tomar las acciones correctivas y/o preventivas, así como comunicar clara y objetivamente los resultados y acciones a todas las partes interesadas.

Finalmente y como opción a futuros trabajos, este diseño se podría ampliar y abarcar los demás procesos que contiene la unidad de negocio de Vivienda, inclusive se podría adaptar a otras unidades de negocio de la inmobiliaria.

Referencias bibliográficas

[AEC, 2012]
Asociación Española para la Calidad
2012 "La norma ISO 27001. Seguridad de la información. Garantía de confidencialidad, integridad y disponibilidad de la información". Revista Calidad. España, Julio 2012, N° III, pp. 40-44.

[APDP, 2013]
Autoridad Nacional de Protección de Datos Personales
2013 La Autoridad Nacional de Protección de Datos Personales APDP: "GUÍA PARA EL CIUDADANO". Primera edición, Octubre 2013.

[CONGRESO DE LA REPÚBLICA DEL PERÚ, 2011]
Congreso de la República del Perú
2011 Ley 29733. Ley de Protección de Datos Personales. Julio 2011.

[DEEPA, KIM y SAMEERA, 2013]
DEEPA MANI, KIM-KWANG, SAMEERA MURABAK
2013 "Information security in the South Australian real estate industry: A study of 40 real estate organisations", Information Management & Computer Security, Vol. 22 Iss: 1, pp.24 - 41

[GESTION, 2013]
2013 "Telefónica del Perú obtiene la certificación ISO 27001" Gestión, el diario de la economía y negocios de Perú. <http://gestion.pe /noticias/telefonica-peru-obtiene-certificacion-iso-27001>

[IRIC, 2013]
2013 "International Register of ISMS Certificates"
ISMS International User Group.
< http://www.iso27001certificates.com/ >

[ISMS, 2013]
2013 ISMS Forum Spain. Asociación Española para el Fomento de la Seguridad de la Información < https://www.ismsforum.es>

[ISO 27001, 2013]
ISO 27001
2013 ISO 27001:2013 Information technology – Security techniques – Information security management systems - Requirements. 2nd Edition

[ISO 27002, 2013]
ISO 27002
2013 ISO 27002:2013 Information technology - Security techniques - Code of practice for information security management. 2nd Edition

[ISO 27003, 2010]
ISO 27003
2010 ISO 27003:2010 Information Technology - Security techniques - Information security management system implementation guidance. 1st Edition

[ISO 31000, 2009]
ISO 31000
2009 ISO 31000:2009 Risk management–Principles and guidelines. 1st Edition

[ISACA, 2012a]
ISACA
2012 “Governance of Enterprise IT (GEIT) Survey” Global Edition, ISACA Consulta: 25 de Abril de 2013 <http://www.isaca.org/GEITSurvey2012>

[ISACA, 2012b]
ISACA
2012 "COBIT 5 for Information Security", USA: ISACA Publishing.

[ISACA, 2013a]
ISACA
2013 “COBIT 5: A Business Framework for the Governance and Management of Enterprise IT” Consulta: 1 de Mayo de 2013 <http://www.isaca.org/cobit5>

[ISACA, 2013b]
ISACA
2013 "Business Model for Information Security (BMIS)" Consulta: 1 de Mayo de 2013 <http://www.isaca.org/bmis>

[ITGI, 2008]
INSTITUTO DE GOBIERNO DE TI
2008 "Information Security Governance: Guidance for Information Security Managers". USA: ITGI Publishing

[LAUDON, 2012]
LAUDON, Kenneth C. y LAUDON, Jane P.
2012 Sistemas de información gerencial. Duodécima edición. México: Pearson Educación.

[MAGERIT, 2012a]
MAGERIT
2012 "MAGERIT 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" Libro I - Método

[MAGERIT, 2012b]
MAGERIT
2012 "MAGERIT 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" Libro III – Guía de técnicas < https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/>

[NORMAS-ISO, 2012]
2012 "NORMAS ISO, Asesoría, Formación y Sistemas de Gestión" Consulta: 03 de Junio de 2013 < http://www.normas-iso.com/iso-27001>

[OMG, 2012]
OBJECT MANAGEMENT GROUP
2012 "Business Process Model and Notation" Object Management Group, Inc. Consulta: 03 de Junio de 2013 < http://www.bpmn.org/>

[PDCA, 2013]
PDCA
2013 "Modelos de acreditación de la calidad" PDCA.España. Consulta: 03 de Junio de 2013 < http://www.pdca.es/>

[PMI, 2013]
PMI Project Management Institute
2013 A guide to the Project Management Body of Knowledge. 5th Edition. Pennsylvania, EEUU. Project Management Institute, Inc.

[PROSEGUR, 2012]
OBJECT MANAGEMENT GROUP
2012 "Ejemplo de Implantación Lecciones Aprendidas de un SGSI" Prosegur Cia de Seguridad S.A <http://www.socinfo.es/contenido/seminarios/seguridadinfo/ >

[PYKA, 2006]
PYKA, Paulina
2006 "The OCTAVE methodology as a risk analysis tool for business resources" Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 485 – 497.Polonia 2006

[SYMANTEC, 2011]
Symantec Corporation
2011 "Reporte sobre Seguridad Empresarial 2011" Consulta: 5 de Mayo de 2013 <http:// www.symantec.com/la/seguridad2011>

[SYMANTEC, 2012]
Symantec Corporation
2012 "Backup Exec 2012" Consulta: 5 de Mayo de 2013 <http:// www.backupexec.com>

[SYSTEMI, 2010]
System Integrity
2010 "The Five Domains of IT Governance"
Consulta: 6 de Mayo de 2013
<http://www.systemi.ca/governance/the-five-domains-of-it-governance>

[TECH, 2010]
Tech Target
2010 "Search Data Center", by Roger Godinho
Consulta: 30 de Mayo de 2013
< http://searchdatacenter.techtarget.com/definition/data-center>

[TUPIA, 2013a]
TUPIA, Manuel
2013 Administración de la Seguridad de Información.
Segunda edición. Lima: Tupia Consultores y Auditores S.A.C

[TUPIA, 2013b]
TUPIA, Manuel
2013 Gestión de Servicios de tecnologías de información bajo la óptica de ITIL V3. Primera edición. Lima: Tupia Consultores y Auditores S.A.C

[RAE, 2001]
REAL ACADEMIA DE LA LENGUA ESPAÑOLA
2001 Diccionario de la Real Academia de la Lengua Española. 22ª edición. España: French & European Publications.

[VILLENA, 2006]
VILLENA, MOISES
2006 "Sistema de Gestión de Seguridad de información para una entidad financiera". Tesis para optar el Título de ingeniero informático. Lima: Pontificia Universidad Católica del Perú. Facultad de Ciencias e Ingeniería. Especialidad de Ingeniería Informática.