PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UNA CENTRAL PRIVADA DE INFORMACIÓN DE RIESGOS

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

Josefina Ríos Villafuerte

ASESOR: Moisés Villena Aguilar

Lima, Junio del 2014

ÍNDICE

Capítulo 1

Capítulo 2

Capítulo 3

Capítulo 4

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPITULO 1: Generalidades

1. Identificación de Problema

Una Central de Riesgo privada está encargada principalmente de brindar información a terceros sobre el nivel de endeudamiento, antecedentes crediticios, comerciales, tributarios, laborales y de seguros de personas naturales y jurídicas, mediante la recolección y procesamiento de información de riesgo con el objeto de evaluar la capacidad de endeudamiento y pago de dichas personas.

El Congreso de la República, emitió en el año 2001 la Ley N°27489 [1], la misma que regula las centrales privadas de información de riesgos y de protección al titular de la información. La cual sería modificada al año siguiente por la Ley N°27863 [2].

El Artículo N°12 de la Ley N°27489 [1] hace referencia a la seguridad de la información, obligando a las Centrales de Riesgo privadas a adoptar medidas de índole técnicas o administrativas que garanticen la seguridad de la información de los titulares, promoviendo la confidencialidad y uso apropiado de dicha información, evitando su alteración, pérdida, tratamiento, o acceso no autorizado.

Asimismo, el capítulo V de la Ley de Protección de Datos personales N°29733 [3], aprobada en Marzo del 2013, establece las medidas de seguridad para el tratamiento de información digital, tales como el respaldo, recuperación y la gestión de acceso de los datos personales.

Surge la necesidad de garantizar que los riesgos de la seguridad de la información sean conocidos, gestionados y minimizados de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías, para brindar un nivel de confianza sobre el cumplimiento de los objetivos del negocio y al mismo tiempo protegiendo la organización.

Un Sistema de Gestión de Seguridad de la Información permite la calidad de la seguridad de la información, gestionando el acceso a la información, brindando confidencialidad, disponibilidad e integridad a la información evitando ataques, filtración, alteración y pérdida de ingresos, cumpliendo con las normas legales.

En este contexto se presenta como propuesta el Diseño de un Sistema de Gestión de Seguridad de Información (SGSI) que permita a una central de riesgos cumplir con la regulación vigente siguiendo normas internacionales actuales.

2. Objetivo General

Diseño de un Sistema de Gestión de la Seguridad de Información (SGSI) el cual permita que una Central de Riesgo Privada pueda cumplir con las exigencias regulatorias a las que se haya sujeta, siguiendo las normas internacionales ISO/IEC 27001:2013, ISO/IEC 27002:2013 e ISO 31000:2009.

3. Objetivos Específicos

- OE1 Modelar los procesos que constituyen el negocio principal de una Central Privada de Información de Riesgos.
- OE2 Identificar y valorar los activos relacionados a los procesos seleccionados.
- OE3 Identificar y evaluar los riegos a los que están expuestos los activos identificados en el punto anterior.
- OE4 Identificar los objetivos de control y controles que son aplicables y relevantes al SGSI de la Central Privada de Información de Riesgos.
- OE5 Elaborar la documentación exigida por la norma adoptada para el diseño del SGSI.

4. Resultados Esperados

- RE1 Modelamiento de los principales procesos de negocio.
- RE2 Lista de activos valorados asociados a los procesos de negocio.
- RE3 Mapa de Riesgos.
- RE4 Declaración de Aplicabilidad, la cual incluya los controles seleccionados y las razones para su elección, objetivos de control, la exclusión de un objetivo de control y la justificación para su exclusión.
- RE5 Según la cláusula 6.1.3, se elaborarán los siguientes documentos del SGSI:
  - Los enunciados de la política de seguridad y objetivos de control.
  - El alcance del SGSI.
  - Plan de Tratamiento de Riesgo.
  - Declaración de Aplicabilidad.
  - Descripción de la Metodología de evaluación del riesgo.

5. Alcance y Limitaciones

5.1. Alcance

Abarcará los principales procesos de una Central Privada de Información de Riesgo:

- Compra de Información

- Venta de Productos y Servicios:
  - Generar Producto por Agencia
  - Generar Producto o Servicio por Web
  - Generar Servicio Complementario :
    - Generar Servicio Etapa Prospección
    - Generar Servicio Etapa Admisión
    - Generar Servicio Etapa Recuperación

5.2. Limitaciones

- Falta de documentación de las principales actividades y procedimientos de la Empresa.

- Acceso limitado a la información de la Empresa para la posterior identificación de riesgos de cada subproceso.

- Falta de disponibilidad de miembros del personal usuario para concretar reuniones y entrevistas.

6. Marco Conceptual

Para el problema planteado y la futura solución es necesario conocer algunos conceptos que se describen a continuación:

6.1. Conceptos relacionados a Seguridad de Información

- **Seguridad de Información**

Preservación de la confidencialidad, integridad y disponibilidad de la información; además también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad. [4]

- **Evento de Seguridad de la Información**

Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de una política de seguridad de la información o una situación previamente desconocida que puede ser relevante para la seguridad. [4]

- **Incidente de seguridad de la información**

Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información. [4]

- **Disponibilidad**

La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada. [4] La información debe encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Es el acceso a la información y a los sistemas por personas autorizadas en el momento que lo requieran, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware y actualizaciones del sistema. Implica también la prevención de ataque de denegación de servicio.

- **Confidencialidad**

La propiedad de que la información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados. [4]
Es el acceso a la información únicamente por personas que cuentan con la debida autorización.

- **Integridad**

Propiedad de salvaguardar por la exactitud y completitud de los activos. [4]
Busca mantener la información libre de modificaciones no autorizadas, de tal manera que se conserve tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

6.2. Conceptos relacionados a Riesgos

- **Riesgo**

Probabilidad de que una amenaza explote una vulnerabilidad del activo, impactando adversamente en la organización.
Combinación de consecuencias de un evento determinado y la probabilidad de ocurrencia asociada. [5]

- **Control**

Medios para gestionar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

6.3. Conceptos relacionados al SGSI

- **Activo**

Cualquier cosa que tenga valor para la organización. [4]

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

Es parte del sistema gerencial general, basado en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. [4]

- **Enunciado de Aplicabilidad**

Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la Organización. [4]

6.4. Definiciones según la Ley y Marco Legal

- **Centrales Privadas de Información de Riesgo (CEPIRS)**

Las empresas que en locales abiertos al público y en forma habitual recolecten y traten la información de riesgos relacionada con personas naturales o jurídicas, con el propósito de difundir por cualquier medio mecánico o electrónico, de manera gratuita u onerosa, reportes de crédito acerca de estas. [2]

- **Información de riesgo**

Información relacionada a obligaciones o antecedentes financieros, comerciales, tributarios, laborales, de seguros de una persona natural o jurídica que permita evaluar su solvencia económica, vinculada principalmente a su capacidad y trayectoria de endeudamiento y pago. [2]

- **Información sensible**

Información referida a las características físicas, morales o emocionales de una empresa natural o a hechos o circunstancias de su vida afectiva o familiar, tales como los hábitos personales, ideologías y opiniones políticas, creencias o convicciones religiosas, estados de salud físicos o psíquicos y la vida sexual u otras análogas que afecten su intimidad y todo lo referido en la Constitución política del Perú en su artículo 2° inciso 6). [2]

- **Titular de la información**

La persona natural o jurídica a la que se refiere la información de riesgos. [2]

- **Reporte de crédito**

Toda comunicación escrita o contenida en algún medio proporcionado por una CEPIR con información de riesgos referida a una persona natural o jurídica, identificada.

- **La Central de Riesgo de Datos**

Conjunto de información de riesgos administrado por la CEPIRS, cualquiera sea la forma o modalidad de su creación, organización, almacenamiento, sistematización y acceso, que permita relacionar la información entre sí, así como procesarla con el propósito de transmitirla a terceros. [2]

- **Fuentes de acceso público**

Información que se encuentra a disposición del público en general o de acceso no restringido, no impedida por cualquier norma limitativa, que está recogida en medios tales como censos, registros públicos, guías telefónicas, etc. [2]

- **Ley 27489 – Artículo N°12: Deber de Seguridad**

"Las CEPIRS deberán adoptar las medidas de índole técnica y administrativa destinadas a garantizar la seguridad de información que manejen, a fin de evitar su alteración, pérdida, tratamiento o acceso no autorizado". [1]

- **Ley 27489 – Artículo N°5: Características**

"Las CEPIRS debe contar, como mínimo, con las siguientes características:
  - Infraestructura adecuada para el debido tratamiento de la información recolectada.
  - Procedimientos internos para una oportuna atención de consultas, quejas y reclamos, cuando sea el caso.
  - Controles internos que proporcionen seguridad en el desarrollo de las actividades, así como procedimientos de validez de la información procesada."

- **Ley 27863 – Artículo N°13: Derechos de los Titulares**

Los titulares de la información registrada en los La Central de Riesgos de datos administrados por las CEPIRS tienen los siguientes derechos:
  - Derecho de acceso a la información de uno mismo.
  - Derecho de modificación y cancelación de la información referida a uno mismo, en caso fuese errónea, inexacta, ilegal o caduca.
  - Derecho de actualización de la información referida a uno mismo. [2]

- **Ley 29733 – Ley de Protección de Datos Personales**

Tiene el objetivo de garantizar el derecho fundamental a la protección de los datos personales y dispone que el Ministerio de Justicia y Derechos Humanos asuman la autoridad Nacional de Protección de Datos personales. [3]
  - Artículo 10 - Principio de Seguridad: Establece que las Compañías deben adoptar las medidas de seguridad que resulten necesarias a fin de evitar la pérdida o alteración por acción humana o medio técnico.
  - Capítulo V – Medidas de Seguridad: En el cual se plantean los artículos para el tratamiento de información digital, gestión de accesos a los

sistemas de información, autenticación de usuarios, privilegios, el respaldo de información y almacenamiento.

6.5. ISO/IEC 27001:2013

Publicada el 25 de Septiembre del 2013 reemplazando a las ISO/IEC 27001:2005. Contiene los requisitos básicos que debe tener todo sistema de gestión de seguridad de la información y es un estándar sobre el cual se certifican los SGSI de las organizaciones.

La nueva estructura de la norma ha sido diseñada con el objetivo de estandarizar todas las normas del sistema de gestión y sus requerimientos funcionales. Adicionalmente, las definiciones han sido relocalizadas en la ISO/ IEC 27000:2012 como referencia normativa.

Adicionalmente, el nuevo estándar se enfoca en la medición y evaluación del desempeño del SGSI en la Organización, mas no en el ciclo Deming del *Plan, Do, Check y Act*, que enfatizaba la anterior norma.

En la Figura 1 se puede apreciar las diferencias de estructura entre las normas 27001:2005 y 27001:2013, mientras que en la Tabla 2 se relacionan las nuevas cláusulas con las etapas del ciclo Deming: Las cláusulas 4, 5, 6 y 7 son un componente de la etapa *Plan* del ciclo Deming, la cláusula 8 es un componente de la etapa *Do,* la cláusula 9 es un componente de la etapa *Check* y la cláusula 10 es un componente de la etapa *Act*.

La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades, objetivos, requerimientos de seguridad procesos y el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo.

Éste estándar es el que los mercados internacionales exigen a las empresas para poder demostrar que la información manipulada está bajo características de confidencialidad, integridad, disponibilidad, y que garantizan continuidad en las operaciones, debido a que cuentan con un sistema para la planificación de la continuidad del negocio. Una empresa con este estándar implantado garantiza, en la cadena de suministros, ser un proveedor confiable.

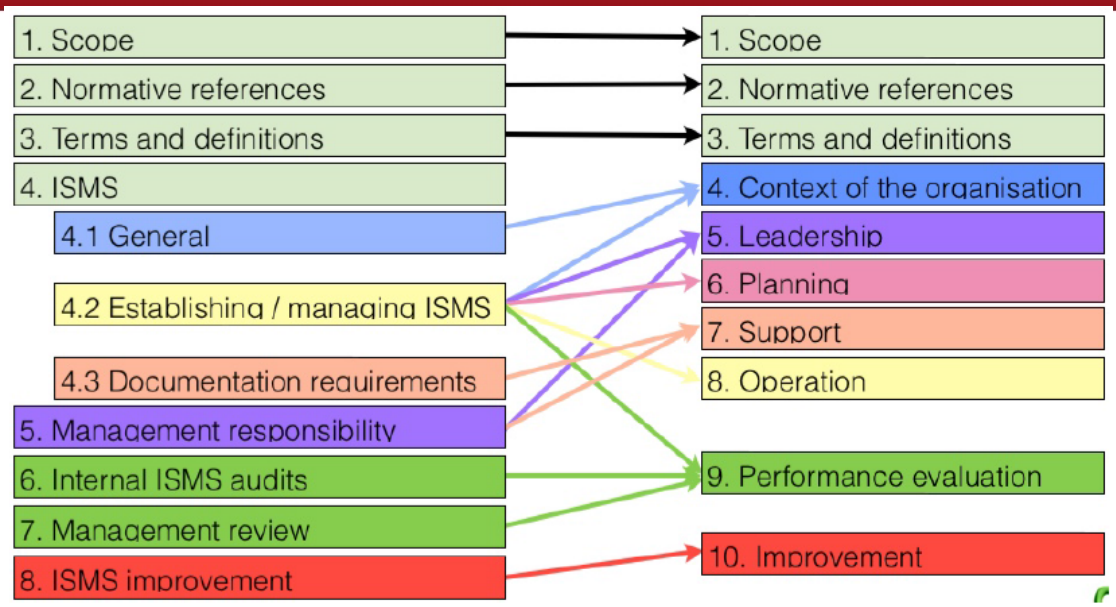


Figura 1. Diferencias estructurales entre las Normas 27001:2005 y 27001:2013 [7]

6.5.1. Alcance

Abarca todo tipo de organizaciones (Por ejemplo: empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). Este estándar Internacional especifica los requerimientos para establecer, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos comerciales generales dentro de la organización. Especifica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella.

El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas.

6.5.2. Aplicación

Los requerimientos establecidos en este Estándar Internacional son genéricos y están diseñados para ser aplicables a todas las organizaciones, sin importar el tipo, tamaño y naturaleza.

Cualquier exclusión de los controles vista como necesaria para satisfacer el criterio de aceptación del riesgo tiene que ser justificada y se debe proporcionar evidencia de que los riesgos asociados han sido aceptados por las personas responsables. Cuando se realizan exclusiones, las aseveraciones de conformidad con este estándar no son aceptables a no ser que estas exclusiones no afecten la capacidad y/o responsabilidad de la organización, para proporcionar seguridad de la información que satisfaga los requerimientos de seguridad determinados por la evaluación de riesgo y los requerimientos reguladores aplicables.

6.6. ISO/IEC 31000:2009 – Gestión del Riesgo en la Seguridad de la Información

La Metodología a utilizar en esta tesis para la gestión de riesgos será este estándar internacional, el cual proporciona directrices para la Gestión de Riesgos en la Seguridad de la Información, apoyando en particular los requisitos planteados en la nueva norma ISO/IEC 27001:2013.

La gestión de riesgos en la seguridad de la información consistirá en el establecimiento del contexto, la identificación y evaluación del riesgo, el tratamiento de riesgo, la comunicación del riesgo y el monitorio y revisión del riesgo.

En la Figura 2 se aprecian los procesos que constituyen la gestión de riesgos propuesta por esta norma.

6.6.1. Comunicación y Consulta

La comunicación y consulta con las partes interesadas externas e internas debe tener lugar durante cada etapa del proceso de gestión de riesgos. Deben abordar cuestiones relacionadas con el riesgo, sus causas, sus consecuencias y las medidas que se están adoptando para tratarlas.
Un enfoque del equipo consultor podrá:

- Ayudar a establecer el contexto adecuado.
- Asegurar que se entiendan y se consideran los intereses de las partes interesadas.
- Ayudar a asegurar que los riesgos se identifican adecuadamente.
- Aportar en diferentes áreas para analizar los riesgos.
- Asegurar que los diferentes puntos de vista sean considerados en la definición de los criterios de riesgo y en la evaluación de riesgos.
- Brindar respaldo y apoyo a un plan de tratamiento.
- Mejorar la gestión del cambio adecuada durante el proceso de gestión de riesgos.
- Desarrollar una comunicación externa e interna y un plan de consulta.

6.6.2. Establecimiento del Contexto

Implica determinar los criterios básicos necesarios para la gestión de los riesgos de la seguridad de la información, definir el alcance, los parámetros internos y externos que se deben tener en cuenta, y establecer un apropiado funcionamiento de la gestión de riesgos de la seguridad de la información en la Organización.

- Contexto Externo: Es el entorno en el cual la Organización trata de lograr sus objetivos, basados en los requerimientos legales y regulatorios, incluyendo al entorno político, financiero, tecnológico, nacional o internacional.
- Contexto Interno: La Gestión del riesgo debe estar alineada con la cultura, procesos, estrategia y estructura dentro de la Organización
- Definir el criterio del riesgo: Los criterios deben reflejar los objetivos de la Organización, algunos serán impuestos por requerimientos legales, sin embargo todos deben ser coherentes con la política de gestión de riesgos de la Organización. Los factores que deben incluir son los siguientes: La naturales y los tipos de causas y consecuencias que pueden ocurrir y cómo van a ser medidos, definición de la probabilidad, opiniones de las partes interesadas, el nivel en el que el riesgo se define como aceptable o tolerable.

6.6.3. Valoración del Riesgo

- **Identificación del riesgo**

La Organización debe identificar las fuentes de riesgo, el impacto, los eventos, sus causas y posibles consecuencias. El objetivo es generar una lista de riesgos sobre la base de eventos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de los objetivos. Esta etapa es la más importante, ya que el riesgo no identificado, no será incluido en el análisis posterior.

- **Análisis del riesgo**

El análisis de riesgos implica el desarrollo de una comprensión de los riesgos para poder determinar si deben ser tratados. Implica la consideración de las causas y fuentes de riesgo, sus consecuencias y la probabilidad de que se puedan producir.

Un evento puede tener múltiples consecuencias, afectando a múltiples objetivos. Los controles existentes, su eficacia y eficiencia también deben tenerse en cuenta. El análisis puede ser cualitativo, semicuantitativo, cuantitativo o una combinación de estos.

Las consecuencias y su probabilidad se pueden determinar a partir del estudio de los eventos. Las consecuencias deben estar expresadas en términos de impacto tangible o intangible.

- **Evaluación del riesgo**

El objetivo de la evaluación del riesgo es ayudar en la toma de decisiones, en base al análisis de riesgos, identificando a los riesgos que necesitan tratamiento y prioridad para la aplicación de este.

La evaluación del riesgo consiste en comparar el nivel de riesgo detectado durante el proceso de análisis con el criterio del riesgo establecido cuando el contexto fue considerado.

Las decisiones deben tomarse considerando los requerimientos legales y reglamentarios, tomando en cuenta el contexto y el grado de tolerancia de los riesgos asumidos por terceros ajenos a la Organización.

6.6.4. Tratamiento del riesgo

Implica la selección de una o más opciones para la modificación de los riesgos y la aplicación de estas opciones. Una vez implementados, el tratamiento proporciona los controles necesarios.

El tratamiento de los riesgos implica lo siguiente:
- Evaluación del tratamiento de riesgos
- Decidir si los niveles de los riesgos residuales son tolerables
- Si no es tolerable, generar un nuevo tratamiento de riesgos
- Evaluación de la eficacia de dicho tratamiento

Las opciones del tratamiento de riesgos no son mutuamente excluyentes en algunas circunstancias, pueden incluir lo siguiente:
- Evitar el riesgo al decidir continuar con la actividad que da lugar al riesgo
- Eliminación de la fuente del riesgo
- Cambiar la probabilidad
- Cambiar las consecuencias
- Compartir el riesgo con otras partes (Financiación del riesgo, contratos con terceros).

Selección de la opción de tratamiento del riesgo

Implica un equilibrio entre los costes y los esfuerzos de aplicación vs. los beneficios que se derivan, en lo que respecta a los requisitos legales, reglamentarios y otros, tales como la responsabilidad social y la protección del medio ambiente.

Las decisiones también deben tener en cuenta la justificación de un tratamiento, por ejemplo en los casos en que el riesgo es alto pero es muy poco probable que ocurra no sería justificable por razones económicas.

Al seleccionar las opciones de tratamiento de riesgos, la Organización debe considerar los valores y percepciones de las partes interesadas y los medios más adecuados para comunicarse con ellos.

Aunque igualmente eficaces, algunos tratamientos de riesgo pueden ser más aceptables para algunos grupos de interés que a otros. El plan de tratamiento debe identificar claramente el orden de prioridad en el que los tratamientos individuales de riesgo deben ser implementados.

El tratamiento del riesgo en sí mismo puede presentar riesgos. Un riesgo significativo puede ser la insuficiencia o ineficacia de las medidas de tratamiento de riesgo. El monitoreo debe ser una parte integral del plan de tratamiento de riesgos para dar garantías de que las medidas siguen siendo eficaces.

El tratamiento del riesgo también puede introducir riesgos secundarios que deben ser evaluados, tratados, controlados y revisados. Estos riesgos secundarios deben ser incorporados en el mismo plan de tratamiento como un nuevo riesgo. El vínculo entre los dos riesgos debe ser identificado y mantenido.

Implementación del Plan de Tratamiento de riesgos

El objetivo es documentar cómo se implementarán las opciones del tratamiento elegido. La información proporcionada en los planes de tratamiento debe incluir lo siguiente:

- Las razones para la selección de las opciones de tratamiento, incluyendo los beneficios que se espera obtener.
- Los responsables de la aprobación del plan y los responsables de la ejecución del plan.
- Acciones propuestas.
- Necesidades de recursos, incluidos los imprevistos.
- Medidas de rendimiento y limitaciones.
- Presentación de informes, y calendario.

Los planes de tratamiento deben integrarse con los procesos de gestión de la organización y discutidos con las partes interesadas pertinentes. Los responsables y las partes interesadas deben ser conscientes de la naturaleza y alcance del riesgo residual después del tratamiento del riesgo. El riesgo residual debe ser documentado y sometido a seguimiento y revisión.

6.6.5. Monitoreo y Revisión del Riesgo

Tanto el monitoreo como la revisión deben ser parte del proceso de gestión de riesgos, cuyas responsabilidades deben estar claramente definidas. Debe contemplar los siguientes aspectos:

- Asegurar que los controles sean eficaces y eficientes tanto en el diseño como en el funcionamiento.
- Obtener más información para mejorar la evaluación de riesgos.
- El análisis y aprendizaje de lecciones de los acontecimientos, cambios, las tendencias, éxitos y fracasos.

- Detectar cambios en el contexto externo e interno, incluyendo cambios en los criterios de riesgo, que puede requerir una revisión de los tratamientos de riesgo.

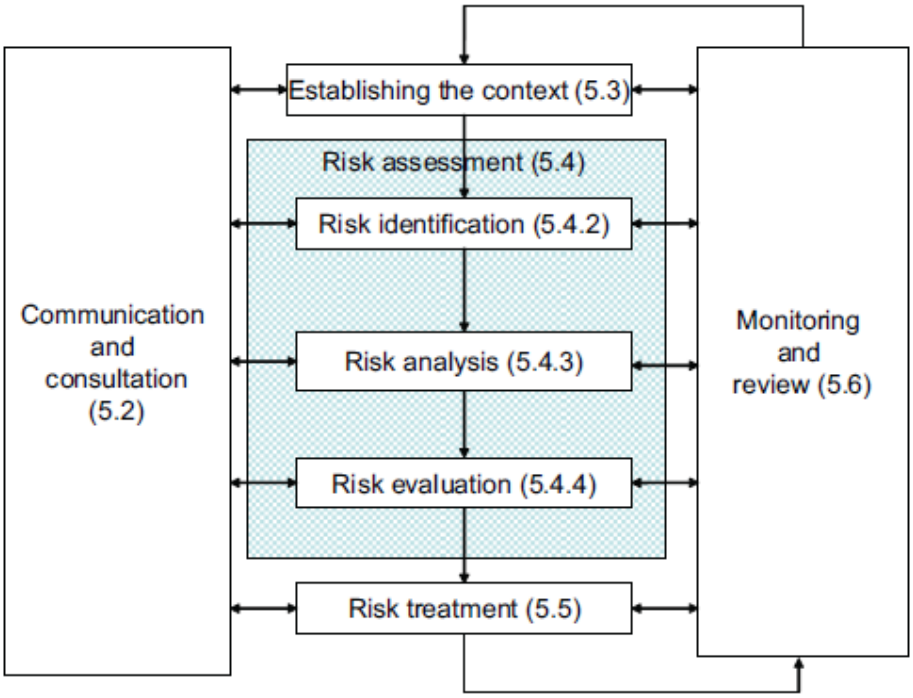


Figura 2. Procesos de la Gestión del Riesgo ISO 31000/2009 [5]

6.7. ISO/IEC 27002: 2013

Publicada el 25 de Septiembre del 2013, reemplazando a la norma ISO/IEC 27002:2005. Describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, contando actualmente con 14 dominios, 35 categorías y 114 controles.

Existen nuevos controles propuestos aplicables a los riesgos que conllevan las nuevas tecnologías, así por ejemplo, en el dominio A.6 Organización de la Seguridad de la Información, se establece la categoría Dispositivos Móviles y Teletrabajo, introduciendo un nuevo control, Políticas de dispositivos móviles.

Los dominios considerados son los siguientes:

- Políticas de la seguridad de la información: Proveen directivas y brindan soporte en la seguridad de información de acuerdo a los requerimientos del negocio y las regulaciones.

- Organización de la Seguridad de la Información: Busca administrar la seguridad dentro de la compañía, así como mantener la seguridad de la infraestructura de procesamiento de la información y de los activos que son accedidos por terceros.

- Seguridad en Recursos Humanos: Orientado a reducir el error humano, ya que en temas de seguridad, el usuario es considerado como el eslabón más vulnerable y por el cual se dan los principales casos relacionados con seguridad de la información. Busca capacitar al personal para que puedan seguir la política de seguridad definida, y reducir al mínimo el daño por incidentes y mal funcionamiento de la seguridad.

- Gestión de Activos: Busca proteger los activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos. Trata que cuenten con un nivel adecuado de seguridad.

- Controles de Accesos: El objetivo de esta sección es básicamente controlar el acceso a la información, así como el acceso no autorizado a los sistemas de información y computadoras. De igual forma, detecta actividades no autorizadas.

- Criptografía: Uso efectivo de la criptografía para proteger la confidencialidad, integridad y disponibilidad de la seguridad de la información.

- Seguridad Física y Ambiental: Trata principalmente de prevenir el acceso no autorizado a las instalaciones para prevenir daños o pérdidas de activos o hurto de información.

- Seguridad de Operaciones: Para asegurar operaciones correctas y seguras en el procesamiento de información.

- Seguridad en las comunicaciones: Esta sección busca asegurar la seguridad cuando la información se transfiere a través de las redes, previniendo la pérdida, modificación o el uso erróneo de la información.

- Adquisición, desarrollo y mantenimiento de los sistemas de información: Básicamente busca garantizar la seguridad de los sistemas operativos, garantizar que los proyectos de TI y el soporte se den de manera segura y mantener la seguridad de las aplicaciones y la información que se maneja en ellas.

- Relación con los proveedores: Gestión de incidentes de seguridad de información: Tiene que ver con todo lo relativo a incidentes de seguridad. Busca que se disponga de una metodología de administración de incidentes, que es básicamente definir de forma clara pasos, acciones, responsabilidades, funciones y medidas correctas.

- Gestión de la continuidad del negocio: Lo que considera este control es que la seguridad de la información se encuentre incluida en la administración de la continuidad de negocio. Busca a su vez, contrarrestar interrupciones de las actividades y proteger los procesos críticos como consecuencias de fallas o desastres.

- Cumplimiento: Busca que las empresas cumplan estrictamente con las bases legales del país, evitando cualquier incumplimiento de alguna ley civil o penal, alguna obligación reguladora o requerimiento de seguridad. A su vez, asegura la conformidad de los sistemas con políticas de seguridad y estándares de la organización.

Nuevos Controles propuestos 27002:2013	
A.6.2.1	Políticas en dispositivos móviles.
A 6.1.5	Seguridad de la Información en la gestión de proyectos.
A.12.6.2	Restricciones en la instalación de software
A.14.2.1	Política de desarrollo de seguridad
A.14.2.5	Desarrollo de procedimientos para sistemas
A.14.2.6	Desarrollo de un entorno seguro
A.14.2.8	Sistema de pruebas de Seguridad
A.15.1.1	Información de seguridad para las relaciones con proveedores
A.15.1.3	Cadena de suministro ICT
A16.1.4	Evaluación y decisión de los eventos de seguridad de información
A16.1.5	Respuesta a incidente de información
A17.1.2	Implementación de la continuidad de la seguridad de la información
A17.2.1	Disponibilidad de instalaciones para procesamiento de información

Tabla1. Nuevos Controles – 27002:2013

6.8. COBIT 5.0

Hoy en día las empresas se enfrentan al gran reto de generar información con valor agregado y 100% confiable, garantizando la seguridad de la información y utilizando tecnologías de información (TI), las cuales permitirán la automatización de los procesos clave del negocio, aumentando la competitividad y permitiendo la innovación, como por ejemplo: La entrega de diferentes productos online. El uso de TI involucra el uso de activos críticos, los cuales deben ser gobernados correctamente.
El uso de las TI significa también hablar de riesgos: la economía en red representa grandes riesgos TI, tales como la no disponibilidad de los sistemas de información, la divulgación de la información de los titulares o clientes, o datos de propiedad, o la pérdida de oportunidades de negocio debido al uso de una arquitectura no flexible lo que conlleva a una negativa reputación y riesgos que pueden poner en peligro la supervivencia de la empresa.
Entonces, la necesidad de gestionar estos y otros tipos de riesgos relacionados con las TI es un motor para un mejor Gobierno de las TI en las empresas (*GEIT-Governance of Enterprise IT* [9]). Su importancia también se le debe atribuir al marco legal con el que deben cumplir algunas empresas, el cual ha llevado a un significativo enfoque en los controles relacionados a las TI. Como también, las infracciones en seguridad de la información pueden conducir a un sustancial impacto a través, por ejemplo, de los daños financieros u operativos.

COBIT 5 apoyará a las empresas a alcanzar sus objetivos, proporcionando un marco integral de referencia y buenas prácticas, el cual permitirá ejercer un gobierno efectivo y una gestión eficiente de las TI, asegurando de que la empresa entregue valor y otorgando confiabilidad en la información a través de los sistemas de información. Se contrarrestarán todos los riesgos involucrados en el reto de generar información 100% confiable.

COBIT 5 permite administrar a las TI de manera integral para toda la empresa, teniendo en cuenta la totalidad del negocio, las áreas funcionales de responsabilidad de las TI y los intereses de las partes interesadas (*stakeholders*), internas y externas, relacionadas con las TI. [9]

COBIT 5 para la Seguridad de la Información se basa en el marco de control COBIT5 y proporciona una guía más detallada para los profesionales en seguridad de la información y los *stakeholders* a todos los niveles de la empresa.

6.8.1. Habilitadores

COBIT 5 incluye los siguientes procesos:

- ***APO13*** *Administración de la Seguridad*
- **DSS04** *Gestión de la Continuidad*
- **DSS05** *Gestión de los servicios de seguridad*

Los mismos que proporcionan una guía básica sobre cómo establecer, operar, y supervisar un SGSI.
Los principales controladores de COBIT para la Seguridad de Información son:

- La necesidad de describir la seguridad de información en un contexto empresarial.
- Una necesidad de la empresa cada vez mayor de: Mantener los riesgos a un nivel aceptable y proteger la información contra la divulgación no autorizada, modificaciones no autorizadas o accidentales y posibles intrusiones; la satisfacción del usuario mediante la disponibilidad de los servicios de TI y el cumplimiento de leyes y reglamentos.
- La necesidad de conectarse, y alinearse con otros importantes marcos y estándares en el mercado.
- La necesidad de unir todas las principales investigaciones de ISACA con un enfoque principal en el Modelo de Negocio de Información de Seguridad (*BMIS*) y COBIT, considerando también *Val IT, Risk IT, IT Assurance Framework (ITAF),* la publicación titulada "*Board Briefing on IT Governance*" y el recurso *Taking Governance Forward (TGF*).

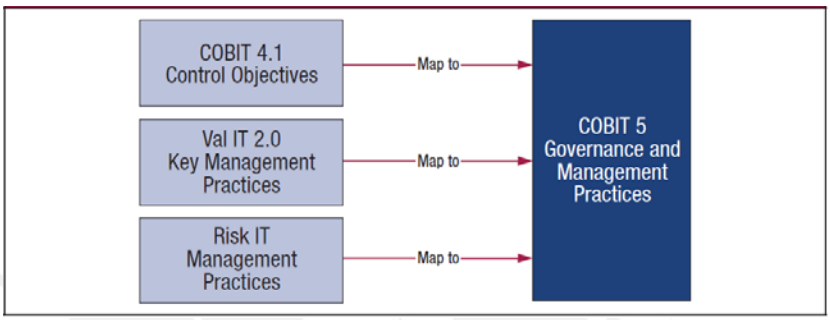


Figura 3. Marco Integral COBIT 5.0 [16]

6.8.2. Beneficios

- Reducción de la complejidad y aumento de la rentabilidad debido a una mayor integración de los estándares de la seguridad de la información.
- Aumento en la satisfacción de los usuarios.
- Integración de la seguridad de la información en la empresa.
- Decisiones a partir de la identificación de los riesgos y Conciencia del riesgo.
- Reducción de los incidentes de la seguridad de la información.
- Mayor apoyo a la innovación y competitividad.
- Mejora de la gestión de costos relacionados con la función de seguridad de la información.

COBIT5 se basa en cinco Principios y siete Habilitadores ("*enablers").* Los principios en los que se basa se identifican en la siguiente figura:

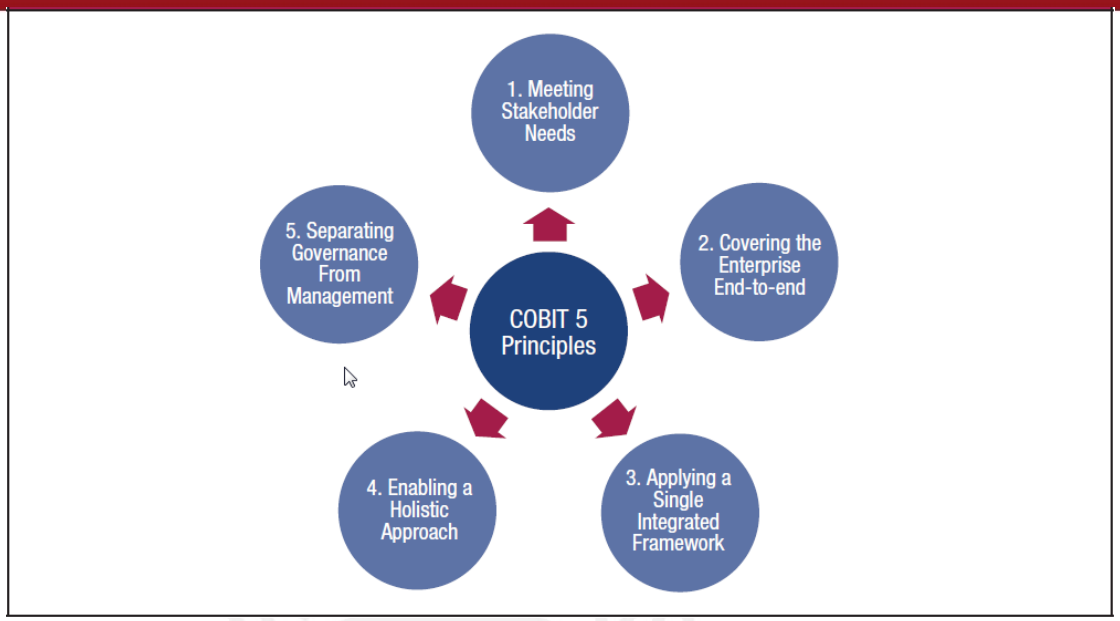


Figura 4. Principios de COBIT 5.0 [16]

6.8.3. Principios

- Satisfacer las necesidades de los *stakeholders*

Dado que cada empresa tiene diferentes objetivos, la empresa debe utilizar la cascada de objetivos para personalizar COBIT5 y adaptarlo a su propio contexto. En la cascada de objetivos, que se presenta en la Figura 4, las necesidades de los *stakeholders* se especifican en los objetivos operacionales de la empresa para ser satisfechos. Estos objetivos de la empresa a su vez requieren objetivos a alcanzar relacionados con los IT, y finalmente se traducen en objetivos para los diferentes facilitadores.

- Abarcar toda la Empresa

COBIT5 cubre todas las funciones y procesos dentro de la empresa que son importantes para la seguridad de información, tratando a la información y tecnología como activos.

- La aplicación de un marco único e integrado

COBIT5 ofrece la posibilidad de integrar eficazmente otros marcos, estándares y prácticas, permitiendo que la empresa lo utilice como un gobierno global y un marco de gestión de TI. Reúne conocimientos de diferentes marcos y modelos de ISACA (COBIT, BMIS, Risk IT, Val IT), series ISO/IEC 27000, *ISF Standard of Good Practice for Information Security* y *U.S. National Institute of Standards and Technology (NIST) SP800-53A.*

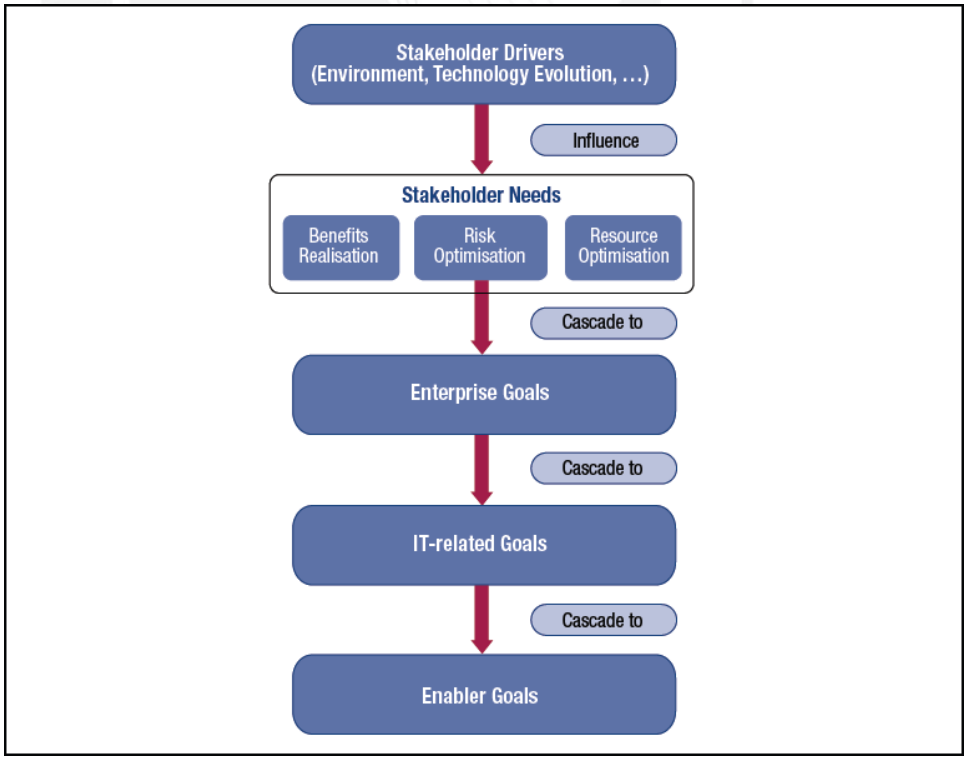


Figura 5. Cascada de Objetivos [16]

- Enfoque integral

Un gobierno eficiente y eficaz y una eficiente gestión de las TI y de la información, requieren un enfoque integral. COBIT5 define un conjunto de facilitadores o factores que influirán en el gobierno y la gestión de las TI y el gobierno de la seguridad de la información, impulsados por la cascada de objetivos.

- Diferenciar Gobierno y Gestión

  - **Gobierno:** Garantiza que las necesidades, condiciones y opciones de los *stakeholders* se evalúen para determinar un equilibrio, logrando los objetivos de la empresa y estableciendo la dirección a través de la toma de decisiones.

  - **Gestión:** Actividades de supervisión, planeamiento, y monitoreo en alineación a la dirección establecida por el gobierno.

  Los Habilitadores, que deben ser considerados para ayudar a promover el logro de los objetivos del marco de la empresa y entregar valor, son:

  1. Políticas de la Seguridad de la Información, principios y marcos.
  2. Procesos y actividades de la seguridad de la información
  3. Estructura organizativa de la seguridad de la información
  4. Cultura, ética y comportamiento como factores que determinan el éxito de la gestión y gobierno de la seguridad de la información.
  5. Gobierno y gestión de la seguridad de la información
  6. Capacidades de servicio necesarias para garantizar la seguridad de la información.
  7. Personas, habilidades y competencias específicas para la seguridad de la información. [16]

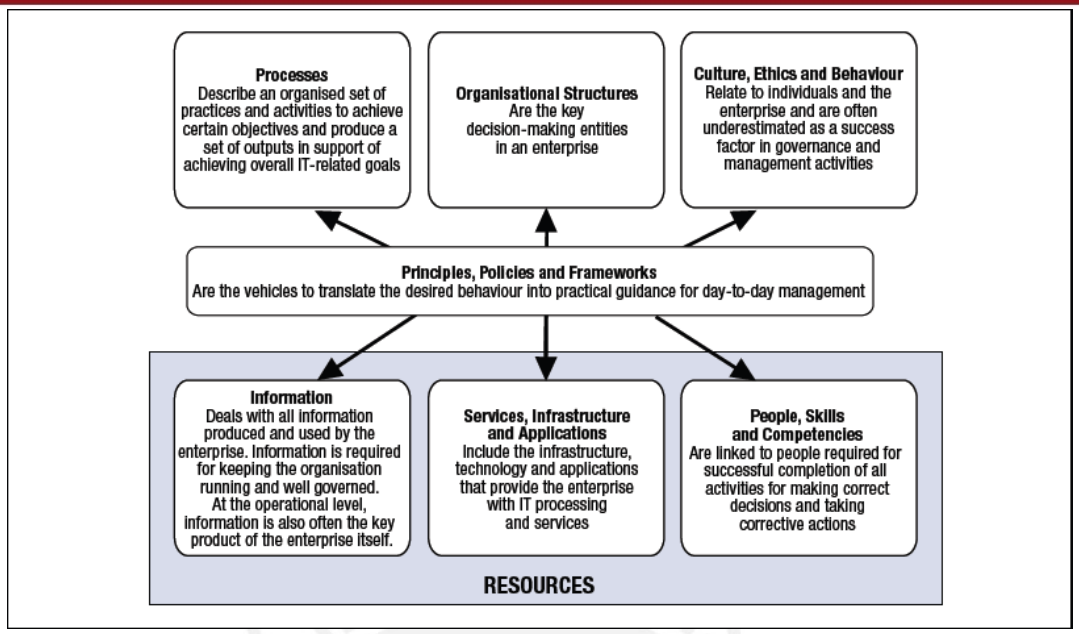


Figura 6 Facilitadores de COBIT 5 [17]

COBIT 5 Incluye procesos que ayudan a guiar la creación y el mantenimiento de la gobernabilidad y Habilitadores de la gestión:

- **EDM01** ***Asegurar el ajuste de un marco de gobierno y su mantenimiento.*** (Cultura, ética y comportamiento, principios, políticas y marcos, estructura organizacional, y procesos).
- **APO01** ***Gestionar el Marco de gestión de TI.*** (Cultura, ética y comportamiento, principios, políticas y marcos, estructura organizacional y procesos).
- **APO03** ***Gestionar la arquitectura de la empresa.*** (Información, servicios, infraestructura y aplicaciones).
- **APO07** ***Gestión de RRHH.*** (Personas, habilidades y competencias).
- **APO2** *Gestionar la Estrategia*

El Gobierno de COBIT5 y los procesos de gestión garantizarán que las empresas organicen sus actividades relacionadas con las TI de manera confiable y repetible. El modelo ahora cuenta con 5 dominios y 37 procesos que forman la estructura para una detallada orientación.

- Ciclo de vida [9]

  Ofrece a las empresas una manera para hacer frente a la complejidad y los desafíos encontrados durante las implementaciones utilizando COBIT5.
  Existen tres componentes interrelacionados:
  - Núcleo: Mejora continua
  - El cambio
  - La gestión del programa

El ciclo de vida abarca siete fases:

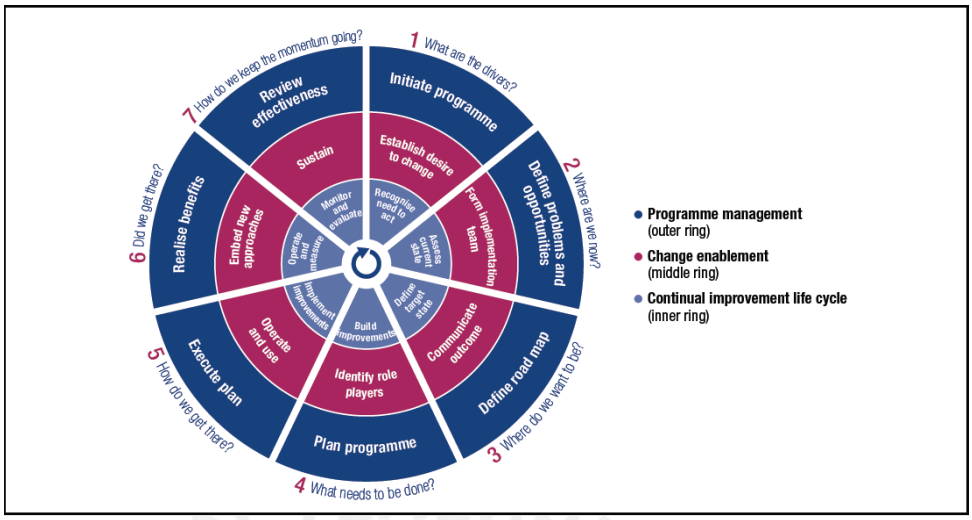


Figura 7 Ciclo de vida [9]

6.9. Risk IT

Publicada en el 2009 por ISACA. La gestión del riesgo empresarial es un componente esencial de la administración responsable de cualquier organización. Debido a su importancia, los riesgos TI deben ser entendidos como riesgos clave para el negocio.

El marco TI permite a los usuarios:

- Integrar la gestión de riesgos IT con el ERM.
- Entender cómo gestionar el riesgo.

Principios:

- Alineación con los objetivos de negocio
- Alineación de la gestión de riesgos de TI con el ERM
- Balancear los costos y beneficios de la gestión de riesgos de TI
- Promover la comunicación justa y abierta de los riesgos de TI

Existen tres dominios en el marco Risk IT:

- Gobierno del Riesgo: Asegura de que las prácticas de gestión de riesgos de TI estén integradas en la empresa, con el objetivo de tener una óptima rentabilidad. Se basa en los siguientes procesos:
  - Establecer y mantener una visión común del riesgo.
  - Integrarlo con el *ERM*
  - Hacer una concientización del riesgo en las decisiones de la empresa.

- Evaluación del Riesgo: Asegurar que los riesgos IT sean identificados y analizados. Se basa en los siguientes procesos:
  - Recopilación de información
  - Análisis del Riesgo
  - Mapa de Riesgos

- Respuesta a los riesgos: Los riesgos deben ser clasificados de acuerdo a las prioridades del negocio:
  - Gestión de Riesgos
  - Implementación de Controles
  - Planes de respuesta a incidentes
  - Comunicación de eventos de risgo. [20]

6.10. M_o_R – Guía para la Gestión de Riesgos

Los principales temas que abarca la Guía son:

- Principios M_o_R: Los principios están alineados con los descritos en ISO 31000, y para ser más consistente con los principios de otras Guías de Gestión.
  Los principios son:
  - Alineación con los objetivos de la empresa.
  - Adaptación con el contexto.
  - Compromiso de las partes interesadas. (*stakeholders*)
  - Proporcionar una orientación clara.
  - Información de las decisiones tomadas.
  - Mejora Continua.
  - Creación de una cultura la cual apoye los principios.
  - Lograr un valor medible.

- Enfoque M_o_R: En donde se encuentra toda la documentación de la Gestión del Riesgo.
- Proceso M_o_R: Hay un gran énfasis a la necesidad de comunicación a lo largo de las diferentes fases del proceso.
  Existen 4 fases:
  - Identificación
  - Activos
  - Plan
  - Implementación

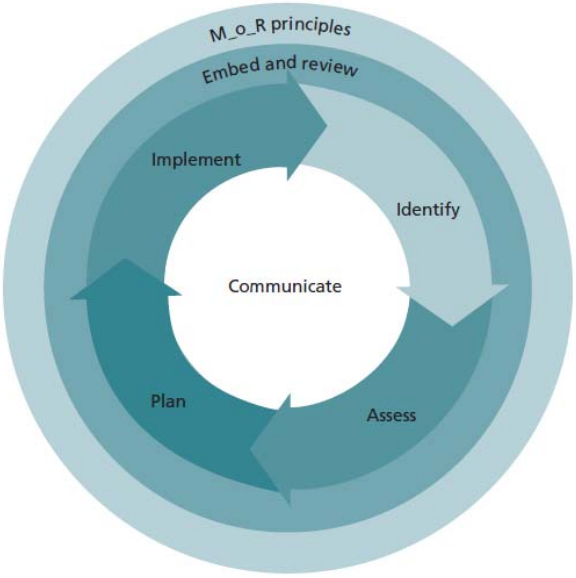


Figura 8 Procesos de Gestión del Riesgo M_o_R [19]

- Revisión M_o_R: Este capítulo ha sido reescrito para mejorar la orientación sobre cómo integrar la gestión de riesgos. [19]

6.11. MAGERIT – Metodología de Análisis y Gestión de Riesgos TI

Desarrollada por el Consejo Superior de Administración Electrónica y publicada por el Ministerio de Administraciones Pública.
La primera versión se publicó en 1997 y la versión vigente en la actualidad es la versión 2.0, publicada en el 2006.

La Metodología consta de tres volúmenes:

- Volumen I – Método: Es el volumen principal en el que se explica detalladamente la metodología.
- Volumen II – Catálogo de elementos: Complementa el volumen principal proporcionando diversos inventarios de utilidad en la aplicación de la metodología. Los inventarios que incluye son:
  - Tipos de activos
  - Dimensiones y criterios de valoración
  - Amenazas
  - Salvaguardas
- Volumen III – Guía de técnicas: Complementa el volumen principal proporcionando una introducción de algunas técnicas a utilizar en las distintas fases del análisis de riesgos. Las técnicas que recoge son:
  - Técnicas específicas para el análisis de riesgos
  - Técnicas Generales [15]

6.12. NIST SP 800-30 Guía de Gestión de Riesgos para Sistemas de Tecnología de Información [7]

El NIST (*National Institute of Standards and Technology*) ha incluido una metodología (*Risk Management Guide for Information Technology Systems*) para el análisis y gestión de riesgos de la Seguridad de la Información, alineada y complementaria con el resto de documentos de la serie.

Compuesta por tres procesos principales: Valoración del riesgo, Mitigación del Riesgo y Evaluación del Riesgo.

- Valoración del Riesgo: Incluye 9 pasos.
  - Paso 1: Caracterización del Sistema
  - Paso 2: Identificación de la amenaza
  - Paso 3: Identificación de una vulnerabilidad
  - Paso 4: Análisis de Control
  - Paso 5: Determinación de la probabilidad
  - Paso 6: Análisis del Impacto
  - Paso 7: Determinación del Riesgo
  - Paso 8: Recomendaciones del Control
  - Paso 9: Resultados de la documentación

- Mitigación del Riesgo: Incluye priorización, evaluación e implementación de los apropiados controles para reducir el riesgo, recomendados del proceso previo.

- Evaluación del Riesgo: En esta etapa se hace hincapié en la buena práctica y la necesidad de una evaluación continua del riesgo y la evaluación y los factores que conduzcan a un programa de gestión de riesgos exitoso.

7. Estado del Arte

7.1. Central de Riesgo en el Reino Unido

En el Reino Unido, la mayoría de La Central de Riesgos y otras organizaciones que conceden créditos se suscriben a una o más Centrales de Riesgo para garantizar la calidad de sus préstamos. Estas Centrales de Riesgo están sujetas a la Ley de Protección de Datos de 1998 ("*Data Protection Act*"), la cual requiere que la información de los titulares sea precisa y relevante. Como también, los consumidores tienen el derecho a solicitar una copia de su expediente crediticio por £2 o acceder vía *online* gratuitamente por un periodo, después del cual se deberá pagar una cuota para el acceso.
Las actividades de las Centrales de Riesgo se rigen por la Ley del Crédito del Consumidor de 1974.

Una de las Centrales de Riesgo más importantes del Reino Unido es CallCredit, creada por Skipton Building Society. La cartera de clientes incluye La Central de Riesgos, telecomunicaciones y empresas de servicio público. Además, de brindar información de riesgo crediticio, brinda soluciones de marketing para la captación de clientes, ayudando a los clientes a gestionar sus relaciones a través de sus productos.

Una de las principales certificaciones de CallCredit es la de ISO/IEC 27001:2005, la cual le permite cumplir con el marco legal impuesto. [21]

Figura 9 . Certificación CallCredit ISO27001 [21]

7.2. Central de Riesgo en Sudamérica

SINACOFI (Sistema Nacional de Comunicaciones Financieras) es una empresa chilena la cual brinda soluciones a Instituciones Financieras, además de contar con una Central de Riesgos. Contempla el desarrollo de actividades relacionadas con el procesamiento de datos mediante sistemas computacionales, sistemas automatizados de transferencia de información y la prestación de servicios de información a la industria bancaria y al mercado en general.

En la prestación de servicios de información tanto a la industria bancaria como al mercado en general, SINACOFI efectúa un tratamiento de datos personales, el cual se encuentra regulado por la Ley N° 19.628 sobre la Protección de la Vida Privada y Tratamiento de Datos Personales, siendo modificada por la Ley N° 19.812 y la Ley N° 19.496 sobre Protección de los Derechos del Consumidor.

La ley N° 19.628 constituye un marco general y particular, a partir del cual, SINACOFI otorga sus servicios de información comercial. En este sentido, la actividad comercial de SINACOFI se debe desarrollar en estricto apego a las

disposiciones de las leyes señaladas, en especial, al tratamiento de la información de los titulares.

SINACOFI implementó un Sistema de Gestión de Seguridad de Información (SGSI) con el objetivo de garantizar a sus clientes confiabilidad y tranquilidad. En Enero, del año 2010 recibe un Certificado en el estándar ISO 27001:2005.

Mediante este certificado, los clientes pueden estar seguros de que su información está resguardada de manera apropiada, y que los servicios son probados y monitoreados permanentemente, cumpliendo asimismo, con el marco legal. [22]

Figura 10. Certificación SINACOFI ISO27001 [22]

7.3. Central de Riesgo en Norteamérica

Las centrales de riesgo en los Estados Unidos están reguladas por la ley Federal *"Fair Credit Reporting Act"*, la cual regula la recolección, difusión y el uso de la información de los consumidores. Es la base de los derechos crediticios del consumidor, haciéndose cumplir por la Comisión Federal de Comercio de los Estados Unidos.

Una de las centrales de riesgo más importantes en dicho país es Experian Information Solutions, Inc. (Experian), ubicada en Orange, California. La compañía provee soporte al negocio de sus clientes, ayudándolos en la gestión de riesgos crediticios, prevención de fraude y marketing. Sus 4 principales líneas de negocio son: Servicio de Información crediticia, Decisiones Analíticas, Servicios de Marketing y Servicio Interactivo.

La seguridad de la información es el core en las operaciones de Experian, ya que se debe enfrentar a un significativo número de riesgos relacionados a la pérdida de información. Asimismo debe manejar data sensible, incluyendo extensas bases de datos en un ambiente totalmente seguro.

El cumplimiento del marco legal, gobierno de la seguridad de información y protección de la información son objetivos de Experian. Para defender la información de los riesgos, Experian ha desarrollado un marco de seguridad basado en la ISO 27001, el cual es la base de las políticas de seguridad implantadas.

Experian cuenta con un Comité de Riesgo Global que apoya la política de Seguridad Global de la Información basada en el Estándar ISO 27001, que cubre:

- Organización y Gestión

- Seguridad de la Información
- Clasificación de Activos
- Seguridad Física y Ambiental
- Comunicaciones y Gestión de Operaciones
- Sistema de Acceso
- Desarrollo de Sistemas y Mantenimiento
- Cumplimiento
- Personal y Aprovisionamiento
- Gestión de la Continuidad de negocio

Las políticas incluyen varias áreas, que van desde la física hasta controles ambientales. Estas áreas requieren controles específicos tales como el uso de Internet. [12]

DET NORSKE VERITAS

MANAGEMENT SYSTEM CERTIFICATE

Certificate No: 39735-2008-AIS-GBR-UKAS

This is to certify that

Experian Group Ltd
Access Control Group

Riverleen House
Electric Avenue
Nottingham
NG80 1RH

has been found to conform to the Information Security Management System Standard:

ISO/IEC 27001:2005

This Certificate is valid for the following product or service ranges:

Account creation and access management for Experian business areas in accordance with the latest version of the Statement of Applicability.

Initial Certification date: 18 November 2005
ISO/IEC 27001:2005
Certification date: 21 February 2007
This Certificate is valid until: 18 November 2011
The audit has been performed under the supervision of:
Rob Howe
Lead Auditor

UKAS
013

Place and date: Barendrecht, 19 December 2008
for the Accredited Unit: DET NORSKE VERITAS CERTIFICATION B.V., THE NETHERLANDS
K.S. Cheung
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.

Figura 11. Certificado ISO/IEC 27001:2005 a Experian [12]

8. Metodología del Producto

El producto continúa adoptando la metodología del ciclo de Deming (*Plan, Do, Check, Act*) según el estándar ISO/IEC 27001:2005, incluyendo las siguientes cláusulas:

8.1. Contexto de la Organización (Planeamiento):

La organización deberá determinar los problemas externos e internos que son relevantes para su propósito y que afectan la capacidad de la organización para lograr el resultado esperado del sistema de gestión de seguridad de la información.

La organización deberá determinar:

- Las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información.
- Los requisitos de estas partes interesadas pertinentes a la seguridad de la información.

La organización debe determinar los límites y aplicabilidad del sistema de gestión de seguridad de la información para establecer su ámbito de aplicación.

Al determinar este ámbito, la organización debe considerar:

- Los problemas externos e internos
- Las interfaces y las dependencias entre las actividades realizadas por la organización y los que son realizados por otras organizaciones.

El alcance deberá estar disponible como información documentada.

8.2. Liderazgo (Planeamiento)

La alta dirección debe demostrar su liderazgo y compromiso con respecto a la información del sistema de gestión de la seguridad a través de:

- Garantizar la política de seguridad de la información y establecer los objetivos de seguridad de la información y su compatibilidad con la dirección estratégica de la organización.
- Garantizar la integración de los requisitos del sistema de gestión de seguridad de la información con los procesos de la organización.
- Velar por que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.
- Comunicar la importancia de una gestión eficaz de seguridad de la información y de adaptación a los requisitos del sistema de gestión de seguridad de la información.
- Garantizar que el sistema de gestión de seguridad de la información alcance su resultado previsto(s).
- Dirigir y apoyar a las personas para contribuir a la eficacia del sistema de gestión de seguridad de la información.
- Promoción de la mejora continua.
- Apoyo a otras funciones de gestión pertinentes para demostrar su liderazgo ya que se aplica a sus áreas de responsabilidad.

La alta dirección debe establecer una política de seguridad de la información que:

- Sea apropiada para el propósito de la organización.
- Incluya los objetivos de seguridad de la información (véase 8.3) o proporcione el marco para establecer los objetivos de seguridad de la información.
- Incluya un compromiso de cumplir con los requisitos aplicables relacionados con la seguridad de la información.
- Incluya un compromiso de mejora continua del sistema de gestión de seguridad de la información.

La política de seguridad de la información deberá:
- Estar disponible como información documentada.
- Ser comunicada dentro de la organización.
- Estar a disposición de las partes interesadas, según corresponda.

La alta dirección debe asignar la responsabilidad y autoridad para:
- Garantizar que el sistema de gestión de seguridad de la información se ajuste a los requisitos de esta norma internacional.
- Informe sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección.

8.3. Planificación (Planeamiento)

Al planificar el sistema de gestión de seguridad de la información, la organización debe considerar los requisitos mencionados en el punto 8.1. y determinar los riesgos y oportunidades que deben ser abordados para:

- Asegurar que el sistema de gestión de seguridad de la información logre su resultado previsto.
- Prevenir o reducir los efectos no deseados

La organización debe planificar:
- Las acciones para hacer frente a estos riesgos y oportunidades y la forma de integrar y poner en práctica las acciones en sus procesos del sistema de gestión de seguridad de la información.
- Evaluar la eficacia de estas acciones.
- Evaluación de riesgos de seguridad de información

La organización conservará información documentada sobre el proceso de evaluación de riesgos de seguridad de información:
- Tratamiento de los riesgos de seguridad de información.
- La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información.
- Deberá seleccionar las opciones de tratamiento de riesgos de seguridad de información adecuados y tener en cuenta los resultados de la evaluación de riesgos.
- Determinar todos los controles que sean necesarios para poner en práctica la opción de tratamiento de riesgos de seguridad de la información elegida.
- Comparar los controles determinados con los del Anexo A y comprobar que no hay controles necesarios se han omitido.
- Producir una Declaración de aplicabilidad que contiene los controles necesarios y la justificación de las inclusiones, si se están aplicando o no, y la justificación de las exclusiones de controles del Anexo A.

- Formular un plan de tratamiento de riesgos de seguridad de información y obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos de seguridad de la información residuales propietarios de los riesgos.
- La organización conservará información documentada sobre el proceso de tratamiento de riesgos de seguridad de información.

La Organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

- Determinar la competencia necesaria de las personas que hacen el trabajo que afecte la información sobre el desempeño de la seguridad.
- Asegurarse de que estas personas son competentes sobre la base de una educación adecuada, capacitación o experiencia
- Tomar las acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas.
- Retener la información documentada apropiada como evidencia de la competencia.

Las personas que hacen el trabajo bajo el control de la organización deben tener en cuenta:

- La política de seguridad de la información.
- Su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de un mejor desempeño de seguridad de información y las consecuencias de que no cumplan con los requisitos del sistema de gestión de seguridad de la información.
- La organización debe determinar la necesidad de las comunicaciones internas y externas pertinentes para la sistema de gestión de seguridad de la información.

8.4. Operación (Hacer)

La organización debe planificar, ejecutar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para poner en práctica las acciones determinadas. La organización debe aplicar también planes para lograr los objetivos de seguridad de la información y mantener la información documentada en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo previsto.

La organización debe controlar los cambios previstos, y revisar las consecuencias de los cambios no deseados, la adopción de medidas para mitigar los posibles efectos adversos, según sea necesario.
La organización debe asegurarse de que los procesos externalizados se determinan y controlan.

La organización debe llevar a cabo las evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se propongan modificaciones importantes. La organización conservará información documentada de los resultados de las evaluaciones de riesgos de seguridad de información.

Asimismo, la organización conservará la información documentada de los resultados de la seguridad de la información tratamiento del riesgo.

8.5. Evaluación del Desempeño (Revisión)

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de seguridad de la información. Asimismo, debe determinar lo que necesita ser monitoreado y medido, incluyendo los procesos de seguridad de la información y los controles.

La alta dirección debe revisar el sistema de gestión de seguridad de información de la organización para asegurarse de su adecuación y eficacia. La revisión por la dirección debe incluir la consideración de:

- El estado de las acciones de las revisiones por la dirección previas.
- Los cambios en los problemas externos e internos que son relevantes para la gestión del sistema de gestión de seguridad de la información.
- La retroalimentación sobre el desempeño de la seguridad de la información, incluyendo la medición de los resultados, el cumplimiento de los objetivos de seguridad de la información, y el estado del plan de tratamiento de riesgos.
- La organización conservará información documentada como evidencia de los resultados de las revisiones por la dirección.

8.6. Mejoramiento (Actuar)

Cuando se produce una no conformidad, la organización deberá:
Reaccionar a la no conformidad, y según sea el caso:

- Tomar medidas para controlar y corregirlo, y hacer frente a las consecuencias.
- Evaluar la necesidad de acciones para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir o producirse en otros lugares, por la revisión de la no conformidad.
- Determinar las causas de la no conformidad, y determinar si existen incumplimientos similares que podrían producirse.
- Poner en práctica las medidas oportunas.
- Revisar la eficacia de las medidas correctivas tomadas, y realizar cambios en el sistema de gestión de seguridad de la información, si es necesario.
- Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.
- La organización conservará información documentada como evidencia de la naturaleza de las no conformidades y de cualquier acción tomada posteriormente, y los resultados de cualquier acción correctiva.

Cláusula	Descripción
4.0	Componente de la etapa *Plan* del ciclo Deming. Introduce los requerimiento necesarios para establecer el contexto del SGSI cualquiera sea el tipo de Organización.
5.0	Componente de la etapa *Plan* del ciclo Deming. Resume los requerimientos específicos del rol de la Alta Gerencia en el SGSI, y como su liderazgo puede articular las expectativas de la Organización.
6.0	Componente de la etapa *Plan* del ciclo Deming. Describe los requerimientos relacionados en el establecimiento de objetivos y principios para el SGSI. La cláusula 6.1.3 establece un plan de tratamiento de riesgos a partir de controles listados en el Anexo A.
7.0	Componente de la etapa *Plan* del ciclo Deming. Apoya las operaciones del SGSI que se relacionan con el establecimiento de la competencia y de la comunicación en forma recurrente con las partes interesadas, a la vez que documenta, controla, actualiza y mantiene la documentación.
8.0	Componente de la etapa *Do* del ciclo Deming. Define los requerimientos del SGSI y determina cómo alcanzarlos, así como la necesidad de realizar evaluaciones de riesgos de seguridad de información e implementar un plan de tratamiento de riesgos.
9.0	Componente de la etapa *Check* del ciclo Deming. Resume los requerimientos necesarios para medir el funcionamiento del SGSI, así como su cumplimiento con la norma internacional, además de las expectativas de la Alta Dirección y su retroalimentación sobre estas.
10.0	Componente de la etapa *Act* del ciclo Deming. Identifica las incidencias aplicando acciones correctivas.

Tabla2. Relación entre las cláusulas de la Norma 27001:2013 y la Metodología Deming

9. Metodología del Proyecto

El proyecto se va a desarrollar siguiendo la metodología PMBOK versión 5. PMBOK cuenta con diez Áreas del Conocimiento, y reconoces 5 grupos de procesos básicos.

Las Áreas del Conocimiento son las siguientes: Gestión de la Integración del Proyecto, Gestión del Alcance del Proyecto, Gestión del Tiempo del Proyecto, Gestión de los Costos del Proyecto, Gestión de la Calidad del Proyecto, Gestión de los Recursos Humanos del Proyecto, Gestión de las Comunicaciones del Proyecto, Gestión de los Riesgos del Proyecto, Gestión de las Adquisiciones del Proyecto y Gestión de los *Stakeholders* del proyecto.

Los Grupos de procesos son los siguientes: Iniciación, Planificación, Ejecución, Seguimiento y Control, Cierre.

Para el desarrollo de este proyecto se abarcaron las Área de conocimiento compuestas por Gestión del Alcance del Proyecto, Gestión del Tiempo del Proyecto y la Gestión de los Riesgos del Proyecto, como lo muestra la Tabla 2.

Áreas del conocimiento	Grupo de Procesos de Gerencia de Proyectos				
	Grupo de Procesos de	Grupo de Procesos de Planificación	Grupo de Procesos de Ejecución	Grupo de Procesos de Seeguimiento y Control	Grupo de Procesos de Cierre
1. Gestión de la Integración del		1.1. Desarrollar la dirección del proyecto.		1.2. Controlar el avance del proyecto.	
2. Gestión del Alcance del Proyecto		2.1. Definir el Alcance 2.2. Crear WBS			
3. Gestión del Tiempo del Proyecto		3.1. Cronograma del proyecto - Gantt	3.2. Definir una Metodología de Gestión de Riesgos 3.3. Análisis de Riesgo 3.4. Mapeo COBIT 5.0	3.5. Controlar el cronograma	
4. Gestión de Costos del Proyecto					
5. Gestión de la Calidad del Proyecto		5.1. Planificar la Gestión de Calidad			
6. Gestión de los RRHH del Proyecto					
7. Gestión de las comunicaciones del Proyecto					
8. Gestión de los riesgos del proyecto		8.1. Identificación y Tratamiento de Riesgos 8.2. Declaración de la Aplicabilidad		8.3. Controlar los riesgos.	
9. Gestión de las adquisiciones del Proyecto					
10. Gestión de los stakeholders del Proyecto			10.1. Gestionar la relación con los interesados.		

Tabla 3. Metodología PMBOK 5

10. Métodos y Procedimientos

Tomando como referencia lo especificado en el estándar ISO IEC 27001:2013, para el establecimiento del SGSI, se define lo siguiente:

1. Identificar los principales procesos de negocio, con los que opera normalmente una compañía de seguros en general.
2. Evaluar la metodología de análisis de riesgo a utilizar para analizar los procesos de negocio.
3. Realizar un análisis de riesgo en cada uno de los procesos identificados, utilizando la metodología escogida.
4. Definir los controles que se ajusten a los procesos identificados, para lo cual se optará por la plataforma de control COBIT 5.0, complementando con los controles de la ISO/IE 27002:2013.
5. Definir una política de seguridad, apoyada en normas, estándares y procedimientos, que den un sustento a los controles seleccionados para cubrir la problemática.

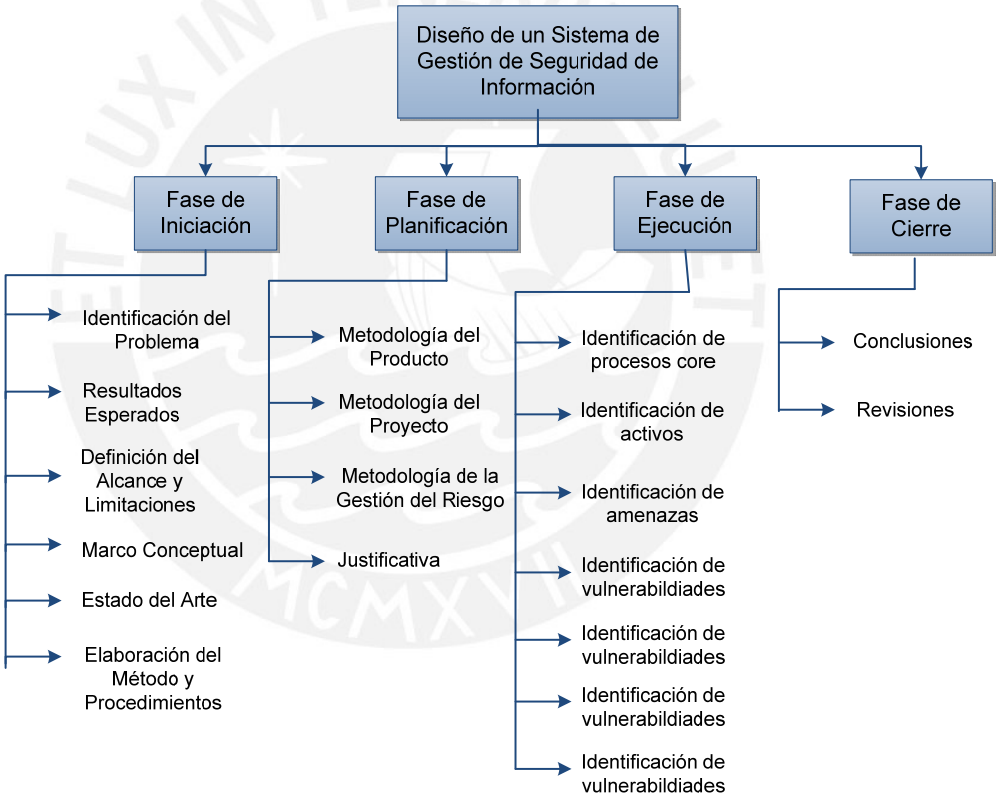
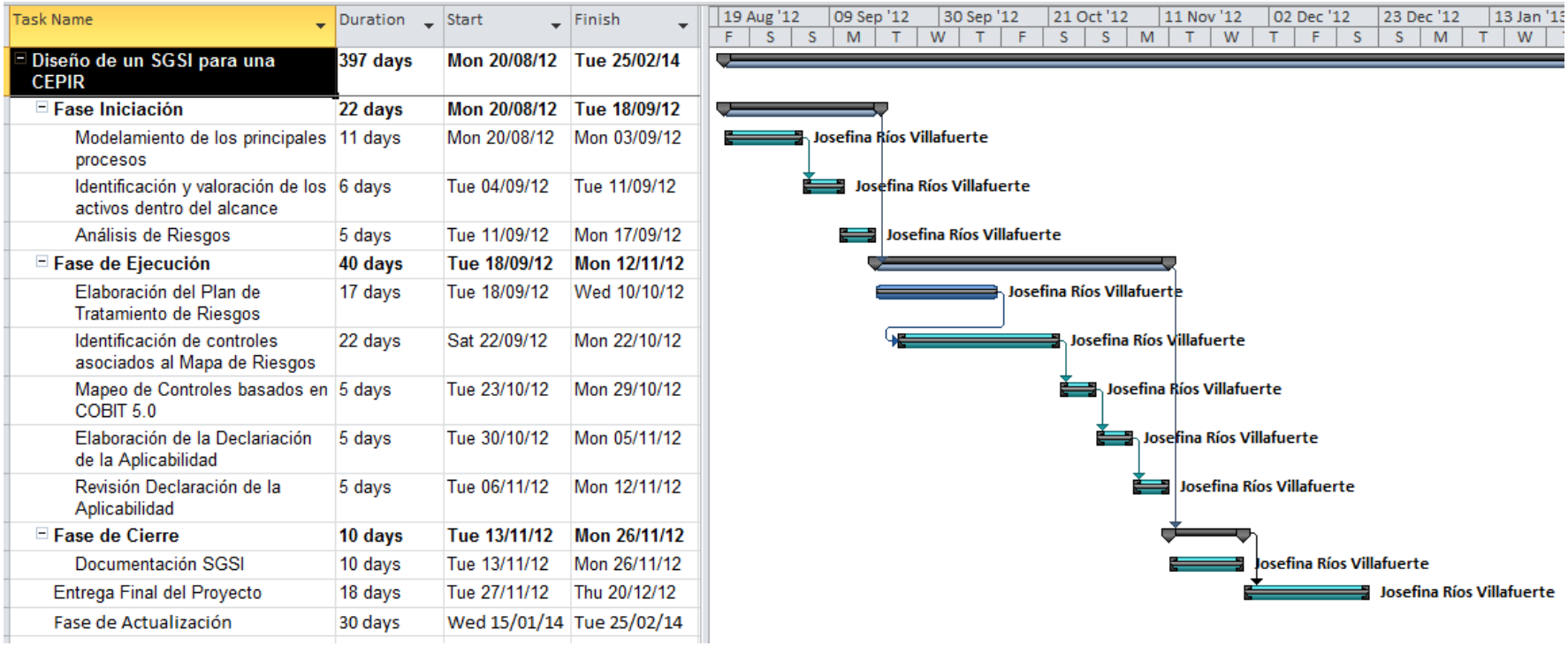


Figura 12. EDT

A continuación el diagrama de Gantt, el cual contiene el Plan de Trabajo para el desarrollo de la Tesis:



Task Name	Duration	Start	Finish
Diseño de un SGSI para una CEPIR	**397 days**	**Mon 20/08/12**	**Tue 25/02/14**
Fase Iniciación	**22 days**	**Mon 20/08/12**	**Tue 18/09/12**
Modelamiento de los principales procesos	11 days	Mon 20/08/12	Mon 03/09/12
Identificación y valoración de los activos dentro del alcance	6 days	Tue 04/09/12	Tue 11/09/12
Análisis de Riesgos	5 days	Tue 11/09/12	Mon 17/09/12
Fase de Ejecución	**40 days**	**Tue 18/09/12**	**Mon 12/11/12**
Elaboración del Plan de Tratamiento de Riesgos	17 days	Tue 18/09/12	Wed 10/10/12
Identificación de controles asociados al Mapa de Riesgos	22 days	Sat 22/09/12	Mon 22/10/12
Mapeo de Controles basados en COBIT 5.0	5 days	Tue 23/10/12	Mon 29/10/12
Elaboración de la Declariación de la Aplicabilidad	5 days	Tue 30/10/12	Mon 05/11/12
Revisión Declaración de la Aplicabilidad	5 days	Tue 06/11/12	Mon 12/11/12
Fase de Cierre	**10 days**	**Tue 13/11/12**	**Mon 26/11/12**
Documentación SGSI	10 days	Tue 13/11/12	Mon 26/11/12
Entrega Final del Proyecto	18 days	Tue 27/11/12	Thu 20/12/12
Fase de Actualización	30 days	Wed 15/01/14	Tue 25/02/14

Figura 13. Diagrama de Gantt

11. Justificación

Hay una serie de razones directas y prácticas para la aplicación de una política de seguridad de la información y un Sistema de Gestión de la Seguridad de la información (SGSI) certificado con el estándar ISO/IEC 27001:2013 en una Central de Información de Riesgos Privada. Un certificado garantiza a los clientes existentes y potenciales que la organización ha definido y puesto en marcha los procesos efectivos de seguridad de la información, ayudando así a crear una relación de confianza. Un proceso de certificación también ayuda a que la organización se centre en la mejora continua de los procesos de seguridad de la información, manteniendo este sistema a la altura y garantizando su capacidad para funcionar.

Asimismo, asegura las medidas técnicas de seguridad para proteger la información. Los sistemas de gestión y los controles de procedimiento son componentes esenciales para que cualquier sistema de información sea realmente seguro y eficaz. La ISO 27001 proporciona la especificación para un Sistema de gestión de Seguridad de Información, el cual se basa en la identificación de activos y la lucha contra toda la gama de riesgos potenciales para la información de la organización, la variedad y el impacto.

Adicionalmente, permite que la Central de Información de Riesgos Privada demuestre que está cumpliendo con los requisitos del gobierno, así como la protección de datos y la legislación sobre privacidad en su jurisdicción local. Igualmente importante, un certificado ISO 27001 permite demostrar a cualquiera de sus clientes que sus sistemas son seguros, y esto, en la economía moderna global de la información, es, por lo menos, tan importante como demostrar el cumplimiento de la legislación local.

La certificación de ISO 27001 del SGSI de la organización es un paso valioso. Es una declaración clara a los clientes, proveedores, socios y autoridades de que la organización tiene un sistema de gestión de la información seguro. [14].

CAPITULO 2: MODELAMIENTO DE PROCESOS E IDENTIFICACIÓN DE ACTIVOS

1. Modelamiento de Procesos

Se elaborará el modelamiento de los principales procesos de una CEPIR.
Ver Anexo 1.

1.1 Venta de Productos y Servicios

1.1.1 Venta por Agencia

Según el artículo 13° de la ley N° 27863 que hace referencia al derecho de los titulares de la información, se refiere a que estos tendrán el derecho de acceso a la información referido a ellos mismos, registrada en los La Central de Riesgos, así como a su modificación o cancelación, rectificación y actualización.

Por tal razón, las centrales de riesgo han implementado espacios de atención al público en general, agencias, en donde puedan acercarse las personas que requieran su información sobre su historial crediticio. Estos reportes son obtenidos de la Base de datos de la central de riesgo, información la cual puede ser corregida en caso se deba limpiar el historial crediticio del titular.

Por ley, el titular tiene derecho a adquirir su reporte crediticio gratis una vez al año y a saber quiénes han consultado su historial crediticio. Si en caso el titular desee adquirir su reporte por una segunda vez, este tendrá un costo, lo mismo que para un tercero.

1.1.2 Venta por Web

El reporte crediticio también puede ser comprado a través del portal de una Central de Riesgo por cualquier persona que desea consultar su propio historial crediticio, o desee saber si la persona o empresa con la que va a hacer negocios cumple son sus obligaciones o si está en capacidad para realizar transacciones comerciales, por ejemplo.

Adicionalmente, el titular también tiene la opción de comprar un servicio basado en “alarmas”, es decir, el cliente recibirá un correo electrónico periódicamente, el cual le informará sobre cualquier modificación en su Reporte crediticio, consultando la siguiente información:

- Calificación y posición de deuda en el sistema financiero.
- Documentos protestados.
- Si lo reportaron como moroso en el sistema financiero, comercial y de servicios.
- Información negativa de SUNAT por omisiones o impagos.

1.1.3 Venta de Servicios Complementarios

En la actualidad, las centrales de riesgo no solo brindan reportes del comportamiento crediticio de personas naturales y jurídicas, sino que además otorgan productos que ayudan a las empresas a realizar negocios o transacciones comerciales, permitiendo la toma de decisiones.

Los servicios se dividen en Servicios Diferidos y *Online* o Tiempo Real. Los servicios Diferidos son aquellos que se entregan luego de un periodo de tiempo determinado al cliente, mientras que los de tipo *Online* deben ser prestados en tiempo real. Se clasifican de acuerdo al ciclo de vida del cliente: Prospección, Venta, Cobranza y Seguimiento.

- **Prospección:** Estos servicios por lo general son de tipo diferido, es decir, el cliente envía la información con determinado perfil a la Central de Riesgo, esta información es validada con la información de las Bases de Datos de la Central y tratada, para luego de un determinado tiempo ser enviada al cliente como servicio.
  Este tipo de servicios permite a los clientes la evaluación de sus propios clientes actuales o potenciales y se aplican a lo largo de todo el ciclo de vida de un crédito, abarcando desde la generación del mismo hasta el proceso de cobranza. Por ejemplo, un cliente podrá pre-evaluar el riesgo esperado de sus potenciales clientes antes de invitarlos a completar una solicitud de crédito. De esta forma, conocerá el ingreso potencial y podrá asignar una línea de crédito acorde a tal variable.
  Asimismo, existen servicios de marketing para la gestión de cartera de clientes, para el control de los actuales, ayudando a detectar potenciales clientes, nichos de crecimiento y análisis de mercado, ofreciendo datos de personas naturales y jurídicas, siendo estos demográficos o descriptivos, de comportamiento crediticio o de riesgo.

- **Admisión:** Una vez identificado los prospectos, se ofrecen productos para cerrar ventas y establecer cuentas de clientes. Estos servicios pueden ser de tipo *online,* como por ejemplo sistemas expertos con puntuación para personas y empresas ayudando a decidir al cliente si aprueba o no el crédito para una determinada persona en tiempo real, hasta servicios de tipo diferido, como los servicios de verificaciones para confirmar datos a través de la visita física al domicilio o centro laboral del postulante al crédito.

- **Recuperación:** En esta etapa se ofrecen productos que agilizan la labor de cobranza a través de notificaciones a personas o empresas que tengan obligaciones vencidas, o productos que muestren reportes de información de las deudas morosas de personas y empresas reportadas por las fuentes. Los servicios son diferidos, por ejemplo, el cliente envía la información de los clientes morosos a la Central de Riesgo, la cual valida dicha información para luego distribuir Cartas de Cobranza. En base a dicha distribución se efectúa un informe con las estadísticas de los resultados (Número de cartas entregadas, Número de cartas sin entregar, #No Habitan, etc.)

- **Seguimiento:** Los servicios ayudan a los clientes a monitorear y revisar constantemente su cartera de clientes, analizando la información de estos e historial de pagos, pudiendo identificar y actuar para minimizar riesgos. Los servicios en esta etapa son de tipo online en su mayoría, permiten consultar la información de determinada persona o entidad en tiempo real.

1.2 Compra de Información:

Las centrales de riesgo recolectan información de riesgo para la Central de Riesgo de datos mediante contratos que pueden ser privados o públicos en donde se establecen acuerdos y se negocian los términos del contrato, como por ejemplo: cuándo será enviada la información, cómo será enviada, ventas de servicios como mecanismo de retroalimentación de la información.

Si bien la carga de información y su respectivo control de calidad pertenecen a las operaciones del día a día de la empresa, son considerados parte de los principales procesos, ya que es de alta importancia que la recepción y tratamiento de dicha información sea eficiente y además requiere un buen desempeño de las aplicaciones usadas para estas actividades.

La carga de información al host es realizada por operadores, los cuales reciben la información de las fuentes públicas y privadas mediante diversas modalidades (archivos digitales en formato Excel, txt o CDs encriptados), para luego realizar el proceso de control de calidad, mediante el cual se valida información.

Las centrales de riesgo obtienen información por endeudamiento financiero y crediticio en el país y en el exterior, riesgos vinculados con el seguro de crédito y otros riesgos de seguro proveniente de las SBS y complementan dicha información de otras fuentes privadas, como por ejemplo con la Sunat, Cámara de Comercio de Lima, etc.

En este proceso las Centrales de Riesgo recolectan la información de fuentes públicas y privadas para luego limpiarla y validarla.

La mayoría de fuentes llegan a ser clientes, las cuales se dividen en:

- Clientes privados: Financieras y Micro Financieras, Telecomunicaciones, Pequeñas y Mediana Empresas (Por ejm: Seguros, AFPs, SEDAPAL, Empresas de Retail, etc.).

- Clientes públicos: SBS (Superintendencia de Banca y Seguros), SUNAT (Superintendencia de banca tributaria), Cámara de Comercio de Lima, Superintendencia de Aduanas (SUNAD).

La información que se recoge incluye reportes consolidados del comportamiento crediticio, letras protestadas, deudas y morosidades de todas aquellas personas que hayan tenido relaciones comerciales, bancarias, laborales y administrativas con estos clientes, es decir, los titulares de la información.

Luego la información es cargada al host, procesada y validada, contrastando su veracidad con otras bases de datos para el control de calidad. Este proceso responde a la necesidad de cumplir con la ley N° 27863, Artículo 9°, la cual exige contar con información lícita, exacta y veraz que responda a la situación actual del titular de la información.

2. Identificación y Valoración de Activos de Información

En el Anexo 2 se presenta el inventario de activos conteniendo las siguientes columnas:

- Activo: Es el nombre del activo o la manera en la que se le identifica en una CEPIR.
- Descripción: Descripción del activo
- Tarea: Tarea del proceso en la que está presente el activo.
- Proceso: Proceso al cual pertenece el activo o en el que participa.
- Tipo: Indica si el activo es primario o secundario.
- Tangible: Indica si el activo es tangible o no.

Ver Anexo 2.

3. Valoración de Activos

Se establecieron criterios para la asignación de un puntaje sobre cada activo, estableciendo escalas de valoración. Esta escala puede ir desde "crítica" hasta "no es relevante", siguiendo una escala cualitativa.

Los criterios fueron establecidos según la ISO 31000:2009, en su anexo A y especificados en la Tabla 4. Por último, se obtendrá como resultado el valor del activo, el cual será la suma de los valores por criterio que obtenga cada uno. Los activos que se tendrán en cuenta para la realización del proyecto serán los que obtengan un valor mayor o igual a 30 de acuerdo al apetito de riesgo de la Central de Riesgo.

En la Tabla 4 se presentarán las siguientes columnas:

- ID: Identificador de activo.
- Activo: Nombre del activo o como se le denomina en el Centro Cultural.
- Disponibilidad: Valor del criterio de disponibilidad del activo.
- Integridad: Valor del criterio de integridad del activo.
- Confidencialidad: Valor del criterio de confidencialidad del activo.
- Valor: Valor cualitativo estimado del activo.

Ver Anexo 2.

ID	Criterios de Valoración de los Activos	Valor			
		Crítico 3	Medio 2	Bajo 1	No es relevante 0
1	**Desempeño del negocio**	Grave deterioro en el desempeño del negocio	Impacto grave en el desempeño del negocio	Impacto moderado en el desempeño del negocio	Sin impacto en el desempeño del negocio
2	**Entrega del Servicio a Clientes**	Impacto Grave para muchos clientes. Incapacidad para prestar el servicio.	Impacto moderado para muchos clientes.	Impacto leve para pocos clientes	Sin impacto para el cliente
3	**Operación Interna**	Alto costo interno adicional. Interrupción permanente de las actividades	Costo moderado. Interrupción prolongada de las actividades	Interrupción breve de las actividades	Sin Alteraciones en la Organización. No genera ningún costo adicional.
4	**Pérdidas Financieras**	Muy Altas Pérdidas	Pérdidas moderadas	Pérdidas leves	Sin Pérdidas
5	**Reputación de la Empresa**	Pérdida del buen nombre y la reputación	Impacto negativo en la reputación de la Empresa	Impacto moderado en la reputación	Sin impacto en la reputación
6	**Intereses comerciales (valor comercial)**	Interés muy grande para la competencia	Alto interés para la competencia	Interés moderado para la competencia	Sin interés para la competencia
7	**Obligaciones legales y Reglamentarias**	Incumplimiento excepcionalmente grave de la ley	Incumplimiento grave de la ley	Incumplimiento moderado de la ley	Sin impacto sobre el cumplimiento
8	**Información del Titular**	Muy grandes brechas asociadas con la información personal. Pérdida de la confianza del cliente	Impacto grave asociado con la información personal.	Impacto moderado en la información personal.	Sin impacto en la información personal.
9	**Obligaciones contractuales**	Incumplimiento excepcionalmente grave de las obligaciones contractuales. Posible cancelación de contratos relevantes	Incumplimiento grave de las obligaciones contractuales. Posibilidad de incurrir en penas relevantes.	Incumplimiento moderado de las obligaciones contractuales. Posibilidad de deterioro de las relaciones con terceros	Sin impacto sobre el cumplimiento
10	**Liderazgo Tecnológico**	Pérdida del liderazgo tecnológico	Alto impacto en la deficiencia del liderazgo tecnológico	Impacto leve en la deficiencia del liderazgo tecnológico	Sin Pérdida del liderazgo tecnológico

Tabla 4 Criterios para la Valoración de Activos

CAPITULO 3: MAPA DE RIESGOS Y TRATAMIENTO DE RIESGOS

1. Matriz de Riesgos

Según la Metodología escogida para la Gestión de riesgos, la ISO 31000:2009, se deben establecer los criterios básicos para la gestión del riesgo. Dentro de estos criterios se encuentran los criterios de impacto y probabilidad de ocurrencia.

Definiéndose a impacto como aquel que afecta en el negocio en caso se llegara a ocurrir determinada amenaza. Para el desarrollo de esta tesis, el impacto va ligado con la disponibilidad del activo. En el caso de la probabilidad de ocurrencia, se refiere a la probabilidad de que ocurra la amenaza en un intervalo de tiempo.

Para ambos conceptos se presenta una escala desde "Muy baja" hasta "Muy alta", a continuación se presentan los criterios tomados:

Probabilidad del escenario de Incidente				
ID	**Valor**	**Descripción**	**Probabilidad**	**Probabilidad recomendada**
1	Muy Baja (muy improbable)	El escenario en mención es muy improbable que ocurra en la empresa. (Aproximadamente una vez al año)	Muy Baja < 10%	0.05
2	Baja (Improbable)	El escenario en mención ocurre ocasionalmente en la empresa. (Aproximadamente de 2 a 10 veces al año)	Baja 10% - < 35%	0.15
3	Media (Posible)	El escenario en mención ocurre eventualmente en la empresa. (Aproximadamente una vez al mes)	Media 35% - < 65%	0.45
4	Alta (Probables)	El evento ocurrirá probablemente. ((Aproximadamente una vez a la semana)	Alta 65% - < 85%	0.70
5	Muy Alta (Frecuente)	Es muy probable que ocurra el evento	85% +	0.90

Tabla 5 Criterios para el cálculo de la Probabilidad del Escenario del Incidente

Impacto producido por el escenario		
ID	**Valor**	**Descripción**
1	Muy Bajo	Los procesos relacionados no se verían afectados y podrían continuar normalmente con su desarrollo.
2	Bajo	Los procesos relacionados se verían afectados y se requeriría de poco menos de una hora para poder continuar con su desarrollo.
3	Medio	Los procesos relacionados se verían afectados y se requeriría de pocas horas para poder continuar con su desarrollo.
4	Alto	Los procesos relacionados se verían amenazados y se requeriría de algunos días para poder continua con su desarrollo.
5	Muy Alto	Los procesos relacionados se verían seriamente impactados o no se llevarían a cabo. Tiempo indefinido superior a una semana para poder continua con su desarrollo.

Tabla 6 Criterios para el cálculo del Impacto

Asimismo, se tomarán los activos valorizados que satisfacen el apetito de riesgo de la central de Riesgo y se realizarán para ellos una identificación de las amenazas y vulnerabilidades correspondientes para dichos activos. Esta asignación se apreciará en la tabla del **Anexo 3** que cuenta con las columnas:

- IDV: identificación de activo en la valorización.
- Activo: Activo de información que satisface exigencias de la valorización de activos.
- Vulnerabilidad: Posible vulnerabilidad del activo.
- Amenaza: Amenaza a la cual está expuesta el activo.
- IDR: Identificación del posible escenario de incidente.
- Causa: Origen del riesgo, relacionada con la/las amenaza/s
- Evento: incidente en la seguridad de la información
- Consecuencia: Relacionada con el impacto
- Riesgo: Consecuencia del escenario.
- Impacto: Valor cualitativo del impacto del escenario de incidente.
- Probabilidad: Probabilidad de ocurrencia del escenario de incidente.
- Valor: Es el valor cualitativo del escenario de incidente obtenido utilizando el enfoque de la norma ISO 31000.

Cada proceso cuenta con una Matriz de Riesgos, la cual consta de la identificación del riesgo, su causa y consecuencia. La causa estará ligada a la(s) amenaza(s), lo que origina que suceda el evento, mientras que la consecuencia está asociada al impacto.

La tabla 7 muestra los 4 niveles de riesgo considerados: Bajo, medio, alto y crítico

	Nivel de riesgo
1,2,3	Bajo
4,5	Medio
6,7	Alto
8,9	Crítico

Tabla 7 Niveles de Riesgo

	Probabilidad de un escenario de incidente	Muy Baja (1)	Baja (2)	Media (3)	Alta (4)	Muy Alta (5)
Impacto en el negocio	Muy Bajo (1)	1	2	3	4	5
	Bajo (2)	2	3	4	5	6
	Medio (3)	3	4	5	6	7
	Alto (4)	4	5	6	7	8
	Muy Alto (5)	5	6	7	8	9

Tabla 8 Niveles de Riesgo según el Impacto vs. Probabilidad de Ocurrencia

2. Plan de Tratamiento

Una vez seleccionados los riesgos se deberán definir controles para reducir, retener, evitar o transferir los riesgos que obtuvieron un nivel crítico o alto y se deberá definir un plan para tratamiento del riesgo.

El plan de tratamiento plasma las expectativas en cuanto a reducción de riesgo. Las opciones para el tratamiento del riesgo se deberían seleccionar en base al costo para implementar estas opciones y los beneficios esperados como resultado de tales opciones.

Los controles pueden brindar los siguientes tipos de protección:
Corrección, eliminación, prevención, minimización del impacto, disuasión, detección, recuperación, monitoreo y concienciación. Durante la selección del control es importante ponderar el costo de adquisición, implementación, administración, operación, monitoreo y mantenimiento de los controles en comparación con el valor de los activos que se protegen.

3. Mapeo con COBIT 5.0

Se aplicará el marco de control de COBIT 5.0, el cual contiene 17 metas genéricas del negocio, de los cuales se han seleccionado los 19 siguientes como aplicables a la Central de Riesgo:

- Valor para las partes interesadas de las Inversiones de Negocio (1)
- Cartera de productos y servicios competitivos (2)
- Riesgos de negocio gestionados (salvaguarda de activos) (3)
- Cumplimiento de leyes y regulaciones externas (4)
- Continuidad y disponibilidad del Servicio de negocio (7)
- Respuestas ágiles a un entorno de negocio cambiante (8)
- Toma estratégica de decisiones basada en información (9)
- Optimización de costes de entrega de servicio (10)
- Optimización de las funcionalidades del negocio (11)
- Personas preparadas y motivadas (16)

En la Figura 14 se muestra el cuadro de las Metas Corporativas de COBIT 5, también llamado cuadro de mando integral CMI = BSC, junto con las relaciones a los tres principales objetivos de Gobierno como son Obtención de Beneficios, Optimización de riesgos, Optimización de recursos. Además incluye una categorización basada en una relación primaria del negocio (P) y una relación secundaria con el negocio (S).

Figure 4—COBIT 5 Enterprise Goals

BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

Figura 14 Objetivos de Gobierno de COBIT 5

La relación de las metas del negocio relacionadas con las metas de TI se muestra en la Tabla 9:

Dimensión del CMI TI	ID	Objetivo Empresarial relacionado a las TI	Objetivo de Negocio
Financiera	1	Alineamiento de las TI con las estrategias del negocio	1,2,8,9,11
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.	4,15
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.	1
	4	Riesgos de negocio relacionados con las TI	3,7,10
	5	Realización de beneficios del portafolio de inversiones y Servicios relacionados con TI	1,2
	6	Transparencia de los costes, beneficios y riesgos de las TI.	10
Cliente	7	Entrega de servicios de TI en línea con los requerimientos del negocio	1,2,8,11
	8	El uso adecuado de aplicaciones, información y tecnología	11
Interna	9	Agilidad de las TI	1,8,11
	10	Seguridad de información. Infraestructura de procesamiento y aplicaciones.	3,4,7,15
	11	Optimización de activos, recursos y capacidades de las TI	1,10
	12	Capacitación y soporte de procesos de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio.	2,11
	13	Entrega de los programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	1
	14	Disponibilidad de información fiable y útil para la toma de decisiones	7,9
	15	Cumplimiento de TI con las políticas internas	15
Aprendizaje	16	Personal de TI competente	3
	17	Cultura de Innovación	2,8

Tabla 9 Objetivos de TI - Gobierno de COBIT 5

CAPITULO 4: DECLARACIÓN DE LA APLICABILIDAD

1. Declaración de la Aplicabilidad

La cláusula 6.1.3 Tratamiento de Riesgos de la seguridad de información de la norma ISO IEC 27001:2013 establece el desarrollo del documento Declaración de la Aplicabilidad que contenga los controles necesarios y la justificación de su inclusión o exclusión, sugeridos en el Anexo A de la ISO/IEC 27002:2013.

La Declaración de la aplicabilidad debe ser un documento conciso que permita ser utilizado por Gerencia y actualizado, así como también es utilizado como principal evidencia ante auditoría en caso la Organización desee certificarse.

La DdA debe documentar si cada control es aplicable y si ya está implementado, obligando a las empresas a realizar sus actividades sistemáticamente.

Ver Anexo 4.

2. Conclusión

Contar con un adecuado SGSI es indispensable para la administración de la seguridad en una organización con alto nivel de complejidad como lo es una Central Privada de información de riesgo, para poder conseguir una mayor eficiencia y garantía en la protección de sus activos de información y en la calidad de la seguridad de la información.

Algunas conclusiones relevantes de la implicancia de la implementación de un SGSI en una Compañía:

- A través de un SGSI se puede abordar efectivamente la implementación de un marco de gobierno de seguridad de información.
- Es una de las mejoras herramientas para la gestión del riesgo y del cumplimiento en seguridad de la información.
- Un SGSI a corto plazo se diseña y establece, en el mediano plazo se implementa y en el largo plazo se mejora y mantiene.
- La certificación es la consecuencia de haber logrado un primer nivel de madurez en el SGSI.
- Es uno de los estándares más aceptados a nivel nacional e internacional y es base de iniciativas de cumplimiento.
- El SGSI necesita implicación de la Dirección y apoyo de toda la Organización.
- La implantación requiere conocimiento de un experto, por lo que la ayuda externa puede ser imprescindible. Asimismo, contar con un área de seguridad de información es muy importante para el seguimiento y mejoramiento del SGSI.

REFERENCIAS

[1] CONGRESO DE LA REPÚBLICA DEL PERÚ
2001 *Ley 27489.* Ley que regula las Centrales privadas de información de riesgos y de protección al titular de la información. 11 de Junio.

[2] CONGRESO DE LA REPÚBLICA DEL PERÚ
2002 *Ley 27863.* Ley que modifica varios artículos de la ley que regula las Centrales privadas de información de riesgos y de protección al titular de la información. 21 de Octubre.

[3] CONGRESO DE LA REPÚBLICA DEL PERÚ
2011 *Ley 29733.* Ley de Protección de Datos personales. 21 de Junio.

[4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2013 "*Information technology - Security techniques - Information security management systems – Overview and Vocabulary".* International Standard ISO/IEC 27000:2012. Switzerland, 2012.

[5] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2009 "*Risk Management – Principles and guidelines" International* Standard ISO 31000:2009. Switzerland, 2009.

[6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2013 "*Information technology - Security techniques - Information security management systems – Requirements".* International Standard ISO/IEC 27001:2013. Switzerland, 2013.

[7] ISACA – INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION
2013 *"Conferencia Isaca Lima Full Day 2013".*

[8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2013 *"Information technology — Security techniques — Code of practice for information security Controls".* International Standard ISO/IEC 27002:2013. Switzerland, 2013.

[9] NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
2002 *"Risk Management Guide for Information Technology Systems"*. National Institute of Standards and Technology Special Publication 800-30. Gaithersburg, 2002, 54 páginas.
<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

[10] ISACA – INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION
2011 *"Planning for and Implementing ISO 27001".* Isaca Journal. Texas, 2011, Volumen 4.pp 1-8.

[11] ISACA – INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION
2012 *"COBIT 5 - Implementation".* ISACA & ITGI (*IT Governance Institute*). Illinois, 2012.

[12] ALBERTO G ALEXANDER
2007 *Diseño y Gestión de un Sistema de Seguridad de Información.* Primera Edición. Ciudad: Bogotá.

[13] EXPERIAN
<http://www.fscs.org.uk/>

[14] EXPERIAN
<http://www.experian.com/corporate/experian-profile.html>

[15] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2008 "IT Governance – A Manager´s Guide to Data Security and ISO 27001/ISO 27002". Alan Calder & Steve Watkins. 4ta Edición.
<http://longhallconsulting.com/downloads/IT%20Governance%20-%20A%20Managers%20Guide%20to%20Data%20Security%20and%20ISO%2027001%20-%20ISO%2027002.pdf>

[16] ISACA – INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION
2012 *"COBIT 5 – For Information Security".* ISACA & ITGI (*IT Governance Institute*). Illinois, 2012.

[17] ISACA – INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION
2012 *"COBIT 5 – Enabling Processes".* ISACA & ITGI (*IT Governance Institute*). Illinois, 2012.

[18] BEST MANAGEMENT PRACTICE
2010 *"M_o_R Brochure".* London 2010.

[19] INSTITUTE OF INTERNATIONAL FINANCE
2011 *"Risk IT and Operations".* McKinsey&Company – 17 de Julio del 2011.

[20] CALLCREDIT
2012 *"Awards and Certifications".*
< http://www.callcredit.co.uk/about-us/awards-and-certifications>

[21] SINACOFI
2011 "Certificaciones"
<http://www.sinacofi.cl/faq-central.asp>

[22] [CONGRESO DE LA REPÚBLICA DEL PERÚ
2002 *Ley 27806.* Ley de Transparencia y acceso a la información. 08 de Agosto.