TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UNA COMPAÑÍA DE SEGUROS

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

Ampuero Chang, Carlos Enrique

ASESOR: Ing. Moisés Villena Aguilar

Lima, Abril del 2011

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Resumen

En la actualidad, con el desarrollo de la tecnología, la información ha tomado mayor fuerza en las empresas, convirtiéndose en la mayoría de los casos en el activo más importante que tienen. Es por esta razón que tienen la obligación de proteger aquella información que es importante para ellas y que tiene relación ya sea con el negocio o con los clientes.

La Superintendencia de Banca, Seguros y AFP, en el 2009, elaboró la circular G140, que estipula que todas las empresas peruanas que son reguladas por este organismo deben contar con un plan de seguridad de información. La presente tesis busca diseñar un sistema de gestión de seguridad de información para una compañía de seguros que cubra lo que pide la circular para evitar problemas regulatorios con este organismo.

Para esto, se utilizarán estándares y buenas prácticas reconocidos mundialmente para poder desarrollar cada una de las etapas del diseño del Sistema de Gestión de Seguridad de Información (SGSI) y así poder tener una base que se pueda implementar en cualquier compañía de seguros. Cabe resaltar que estos estándares y buenas prácticas indican qué es lo que se debe realizar, pero no especifican cómo se deben implementar los controles. Estos van a depender de la necesidad de la empresa y de la inversión que desee realizar en temas de seguridad, con lo que se puede afirmar que lo expuesto en la tesis es una forma de como se puede diseñar un SGSI.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

DEDICATORIA

A mis padres, por todo el amor y apoyo que me han brindado a lo largo de toda mi vida. Gracias por todo el tiempo y esfuerzo que han invertido en mi para poder ser una mejor persona.

A Kleins, por todo el apoyo e inspiración que me ha brindado para poder terminar esta tesis y por todo el amor que me brinda día a día. Gracias por estar siempre ahí y hacer que cada día que pasa sea uno mejor que el otro solo porque te tengo a mi lado; de no haber sido por ti es probable que todavía no hubiera terminado este documento.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

AGRADECIMIENTOS

Al Ing. Moisés Villena por su asesoría y apoyo en la elaboración de la presente tesis.

Al Ing. César Aguilera por su valioso aporte en el desarrollo de este documento.

Al Ing. Luis Flores por su valioso aporte en el desarrollo de este documento.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Índice de Contenido

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Índice de Ilustraciones

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Índice de Tablas

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Introducción

Actualmente nos encontramos en una época en la que la información y los datos poseen una importancia decisiva en la gran mayoría de compañías, convirtiéndose así en uno de sus activos más importantes. De igual forma, la tecnología actualmente permite la circulación ilimitada de información a través de las redes locales y de Internet, además permite compartir datos y realizar operaciones en forma remota, potenciando la productividad de las personas. Es difícil encontrar un negocio que se haya encontrado al margen de la tecnología de información y que no dependa de la información que procesa.

Si bien es cierto esto es muy importante para las compañías ya que les permite un mayor desarrollo, por contrapartida se tiene la aparición de nuevos riesgos, que van a afectar directamente a aquello que le da valor a toda compañía: su información. Los delitos informáticos se han vuelto la opción de un creciente grupo de delincuentes discretos que hacen uso de la tecnología emergente de manera inapropiada.

Es por esta razón que las compañías han comenzado a tomar conciencia y a proteger aquellos recursos de información que son cruciales para ellos,

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

buscando así brindar una protección adecuada sobre estos recursos. Para ello, las distintas empresas buscan asegurar la integridad, confidencialidad y disponibilidad de la información.

La seguridad puede ser afectada a través de cualquiera de sus tres componentes: el uso indebido de la tecnología, la falta de procesos de planificación de seguridad o el desconocimiento de las personas acerca de las distintas medidas de seguridad informática. La implementación de un sistema de gestión de seguridad de información permite a las empresas poder identificar los riesgos que atenten contra los recursos de la compañía y tratar de mitigarlos, implementando ciertos controles capaces de brindar un nivel aceptable de seguridad.

En conclusión, la seguridad no es un juego y requiere darle la importancia necesaria, contratando expertos o una empresa dedicada a brindar servicios de seguridad que desarrollen un plan para asegurar la información de la empresa, ya que así se evitarán mayores costos operativos, baja productividad, pérdida de información y de dinero, logrando de esta manera asegurar la continuidad del negocio con una seguridad aceptable.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

1. Estado del arte del problema

1.1. Identificación del problema

Desde el primer ataque informático registrado en el año 1989 a la actualidad, no solo ha cambiado la manera como los delincuentes cibernéticos perpetran sus ataques, sino también la motivación que los lleva a cometer este tipo de actos. Hace años, el propósito era hacer daño y adquirir fama, hoy buscan dinero y datos personales. Hay que tener en cuenta que una compañía de seguros cuenta con bastante información relacionada a sus clientes que puede ser de utilidad para que un atacante pueda perpetrar un atentado contra ellos. Y por si fuera poco, las empresas no solo deben preocuparse por posibles ataques internos ya que siempre queda abierta la posibilidad de un ataque interno por un trabajador disconforme. Un ataque simple puede originar daños catastróficos a una empresa si es que no cuenta con controles que mitiguen la probabilidad de ocurrencia de estos. Es en este punto donde surge la necesidad de contar con un Sistema de Gestión de Seguridad de Información para mitigar, no solo distintas modalidades de ataques, sino también casos de fuga de información, modificación indebida, entre otros casos que pueden realizarse, brindando un nivel aceptable de seguridad.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Adicionalmente, a la fecha el ente regulatorio peruano para las entidades financieras, seguros y empresas privadas de sistemas de pensiones, la Superintendencia de Banca, Seguros y AFP (SBS), ha emitido normas relacionadas a la gestión de riesgos de operación, gestión de seguridad de información y gestión de continuidad de negocios. Las empresas reguladas por la SBS vienen destinando los medios y esfuerzos necesarios para alinearse a la normativa [1], la misma que está basada en el estándar internacional ISO/IEC 27001:2005 [2].

Bajo este contexto, se presenta como propuesta un diseño de un Sistema de Gestión de Seguridad de Información, que se encuentra alineado a lo exigido por la norma de gestión de seguridad de información, el cual podrá ser usado como base por cualquier compañía de seguros peruana, para adecuarlo y complementarlo a su operativa particular.

1.2. Marco Conceptual

A continuación se presentan algunas definiciones importantes relacionadas al SGSI que se busca diseñar.

1.2.1. Información

Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. La información, ya sea impresa, almacenada digitalmente o hablada, actualmente es considerada como un activo dentro de las compañías y que se debe proteger, ya que es de gran importancia. [13]

1.2.2. Riesgo

Se define como cualquier impedimento, obstáculo, amenaza o problema que pueda impedirle a la empresa que alcance un objetivo. Se puede ver también como la posibilidad de sufrir un daño o pérdida. Se mide en términos de impacto y probabilidad de ocurrencia. [3] Adicionalmente, para el caso de las compañías de seguro, se puede definir como el monto que están dispuestas a perder en caso se dé una catástrofe.

Tesis publicada con autorización del autor
No olvide citar esta tesis

1.2.3. Administración de riesgos

Se llama así al proceso de identificación, análisis y evaluación de riesgos. [3]

1.2.4. Seguridad de la Información

Es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas. [2]

1.2.5. Sistema de Gestión de Seguridad de la Información (SGSI)

Un SGSI o ISMS, de sus siglas en inglés (*Information Security Management System*), es la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitorea, revisa, mantiene y mejora la seguridad de la información. [2]

1.2.6. Control

El control es un proceso por el cual la administración verifica si lo que ocurre concuerda con lo que supuestamente debe ocurrir. Permite que se realicen los ajustes o correcciones necesarias en caso se detecten eventos que escapan a la naturaleza del proceso. Es una etapa primordial en la administración, pues, por más que una empresa cuente con magníficos planes, una estructura organizacional adecuada y una dirección eficiente, no se podrá verificar la situación real de la organización si no existe un mecanismo que verifique e informe si los hechos van de acuerdo con los objetivos. [13]

1.2.7. Declaración de aplicabilidad

La declaración de aplicabilidad o SOA, del inglés *Statement of Applicability*, Es un documento que se referencia en la cláusula 4.2.1j del estándar ISO/IEC 27001 y describe los objetivos de control y controles relevantes y aplicables al alcance del SGSI de la empresa, en función de la política y conclusiones del proceso de evaluación y tratamiento del riesgo. En el documento básicamente van 2 campos: uno donde va el control específico y una columna donde va la aplicabilidad, donde se justifica la decisión tomada sobre si el control es aplicable o no. [2]

Tesis publicada con autorización del autor
No olvide citar esta tesis

1.2.8. Oficial de Seguridad

Persona encargada de administrar, implementar, actualizar y monitorear el SGSI.

1.3. Marco de referencia

Con el pasar de los años la seguridad de información ha tomado una mayor importancia, lo que trajo consigo que un grupo de especialistas a nivel mundial en temas relacionados a seguridad, riesgos y temas afines, desarrollen diversos marcos de trabajo, metodologías, estándares, buenas prácticas, distintos modelos para diseñar un SGSI, leyes, normativas, entre otros, con la finalidad de brindar a las empresas la oportunidad de adoptarlas y proteger adecuadamente la información de sus clientes. Este capítulo busca explicar a groso modo parte de todo aquello que se ha desarrollado hasta el momento, que guarda relación con temas de seguridad y con el desarrollo de la tesis.

1.3.1. COBIT 4.1

COBIT [4] es un framework (también llamado marco de trabajo) de Gobierno de TI y un conjunto de herramientas de soporte para el gobierno de TI que les permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio.

Describe como los procesos de TI entregan la información que el negocio necesita para lograr sus objetivos. Para controlar la entrega, COBIT provee tres componentes claves, cada uno formando una dimensión del cubo COBIT, que se puede apreciar en la Figura 1.

Como un *framework* de gobierno y control de TI, COBIT se enfoca en dos áreas claves:

- Proveer la información requerida para soportar los objetivos y requerimientos del negocio.
- Tratamiento de información como resultado de la aplicación combinada de recursos de TI que necesita ser administrada por los procesos de TI.

Tesis publicada con autorización del autor
No olvide citar esta tesis

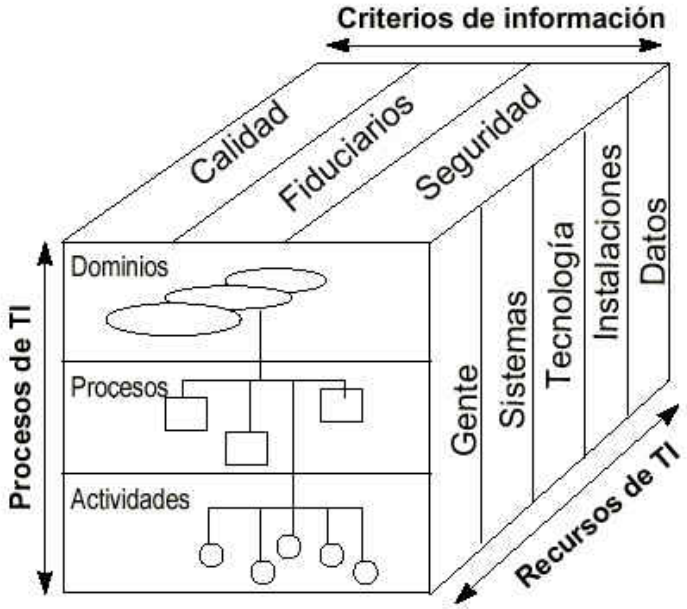

Figura 1. Cubo de COBIT [4]

Tiene 34 procesos de alto nivel clasificados en cuatro dominios: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte, y, Monitorear y Evaluar, tal y como se puede apreciar en la Figura 2.

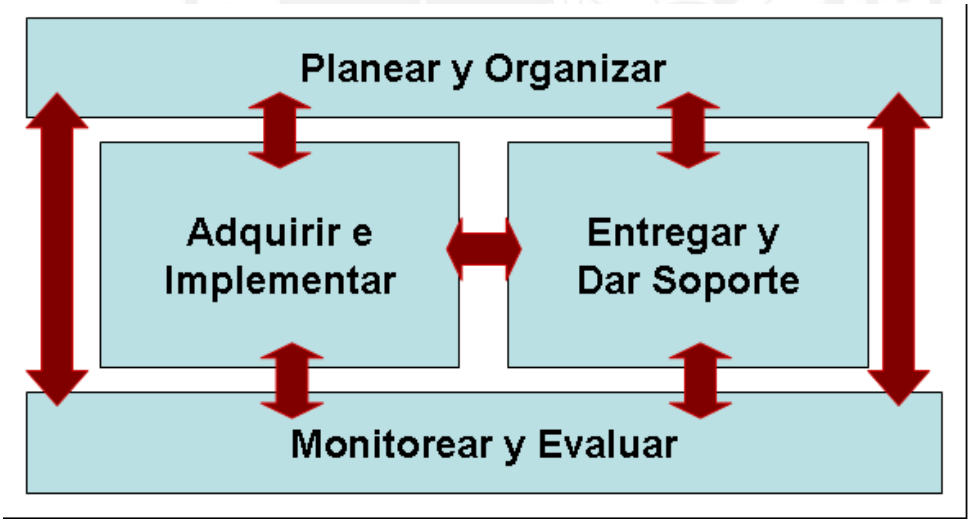

Figura 2. Dominios de COBIT [4]

Tesis publicada con autorización del autor
No olvide citar esta tesis

La misión de COBIT es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores."

COBIT brinda buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica, y están más enfocadas al control y mucho menos en la ejecución. El modelo COBIT cuenta con 4 dominios, 34 procesos de TI, 210 objetivos de control y 40 guías de auditoría. Los 4 dominios de COBIT son:

- **Planear y Organizar:** Este dominio cubre las estrategias y se refiere a la forma en que la tecnología de información puede contribuir a que se cumplan los objetivos del negocio. Busca establecer una organización y una infraestructura tecnológica apropiadas. Los procesos de TI con los que cuenta este dominio son:

  - Definir un Plan Estratégico de TI
  - Definir la Arquitectura de la Información
  - Determinar la Dirección Tecnológica
  - Definir los Procesos, Organización y Relaciones de TI
  - Administrar la Inversión en TI
  - Comunicar las Aspiraciones y la Dirección de la Gerencia
  - Administrar Recursos Humanos de TI
  - Administrar la Calidad
  - Evaluar y Administrar los Riesgos de TI
  - Administrar Proyectos

- **Adquirir e Implementar:** Las soluciones deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio para llevar a cabo la estrategia de TI. Este dominio cubre los cambios y el mantenimiento realizado a sistemas existentes. Los procesos de TI con los que cuenta este dominio son:

  - Identificar soluciones automatizadas.
  - Adquirir y mantener software aplicativo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

- Adquirir y mantener infraestructura tecnológica.
- Facilitar la operación y el uso.
- Adquirir recursos de TI.
- Administrar cambios.
- Instalar y acreditar soluciones y cambios.

- **Entregar y Dar Soporte:** Este dominio hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, seguridad y continuidad. Incluye el procesamiento de los datos por sistemas de aplicación, clasificados frecuentemente como controles de aplicación. Los procesos de TI con los que cuenta este dominio son:

  - Definir y administrar los niveles de servicio.
  - Administrar los servicios de terceros.
  - Administrar el desempeño y la capacidad.
  - Garantizar la continuidad del servicio.
  - Garantizar la seguridad de los sistemas.
  - Identificar y asignar costos.
  - Educar y entrenar a los usuarios.
  - Administrar la mesa de servicio y los incidentes.
  - Administrar la configuración.
  - Administrar los problemas.
  - Administrar los datos.
  - Administrar el ambiente físico.
  - Administrar las operaciones.

- **Monitorear y Evaluar:** Este dominio hace hincapié a que los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control. Los procesos de TI con los que cuenta este dominio son:

  - Monitorear y evaluar el desempeño de TI.
  - Monitorear y evaluar el Control interno.
  - Garantizar el cumplimiento regulatorio.
  - Proporcionar el gobierno de TI.

Tesis publicada con autorización del autor
No olvide citar esta tesis

COBIT a su vez, tiene 7 criterios de información, agrupados en 3 requerimientos (calidad, fiduciarios y seguridad) con los que clasifica a cada uno de los 34 procesos de TI, según el enfoque que tenga el proceso. Estos criterios son:

- **Efectividad:** Se refiere a la información cuando es entregada de manera correcta, oportuna, consistente y usable.

- **Eficiencia:** Se refiere a la provisión de información a través de la utilización óptima de los recursos.

- **Confidencialidad:** Se refiere a la protección de la información sensible de su revelación no autorizada. Tiene que ver que con la información enviada a una persona debe ser vista solo por esa persona y no por terceros.

- **Integridad:** Se refiere a que la información no haya sufrido cambios no autorizados.

- **Disponibilidad:** Se refiere a que la información debe estar disponible para aquellas personas que deban acceder a ella, cuando sea requerida.

- **Cumplimiento:** Se refiere a cumplir con las leyes, regulaciones y acuerdos contractuales a los que la compañía se encuentra ligada.

- **Confiabilidad:** Se refiere a la provisión de la información apropiada a la alta gerencia que apoyen a la toma de decisiones.

En todos los procesos de TI del COBIT se puede saber a qué enfoque está orientado. Puede ser que abarque todos los enfoques, o que sólo abarque algunos, y para todos los controles se indicará si el enfoque es primario (P) o secundario (S).

Tesis publicada con autorización del autor
No olvide citar esta tesis

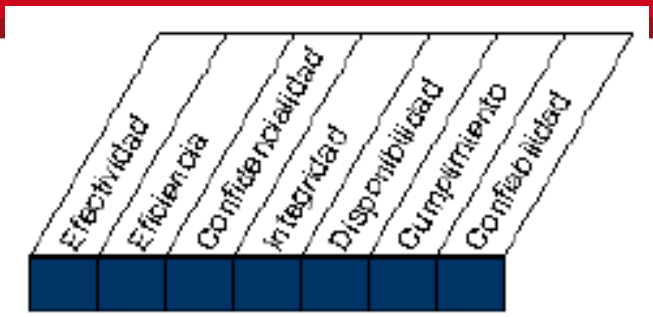

Figura 3. Enfoque de procesos de TI de COBIT [4]

Con respecto a los recursos de TI mencionados en la otra dimensión del cubo, se definen de la siguiente manera:

- Aplicaciones: Son procedimientos manuales y sistemas de usuarios automatizados que procesan información.
- Información: Es data que son ingresada, procesada y obtenida de los sistemas de información en cualquier formato usado por el negocio.
- Infraestructura: Incluye la tecnología y facilidades tales como: hardware, sistemas operativos y redes que permiten el procesamiento de las aplicaciones.
- Personas: Son requeridos para planificar, organizar, adquirir, implantar, entregar, soportar, monitorear y evaluar los servicios y sistemas de información. Ellos podrían ser internos, outsourcing o contratado

1.3.2. AS/NZS 4360:2004

Desarrollada por australianos y neozelandeses, es una metodología que permite administrar los riesgos. Especifica los elementos del proceso de administración de riesgos, independientemente del tipo de empresa. A continuación, en la Figura 4, se puede apreciar el ciclo de vida de la metodología:

Tesis publicada con autorización del autor
No olvide citar esta tesis

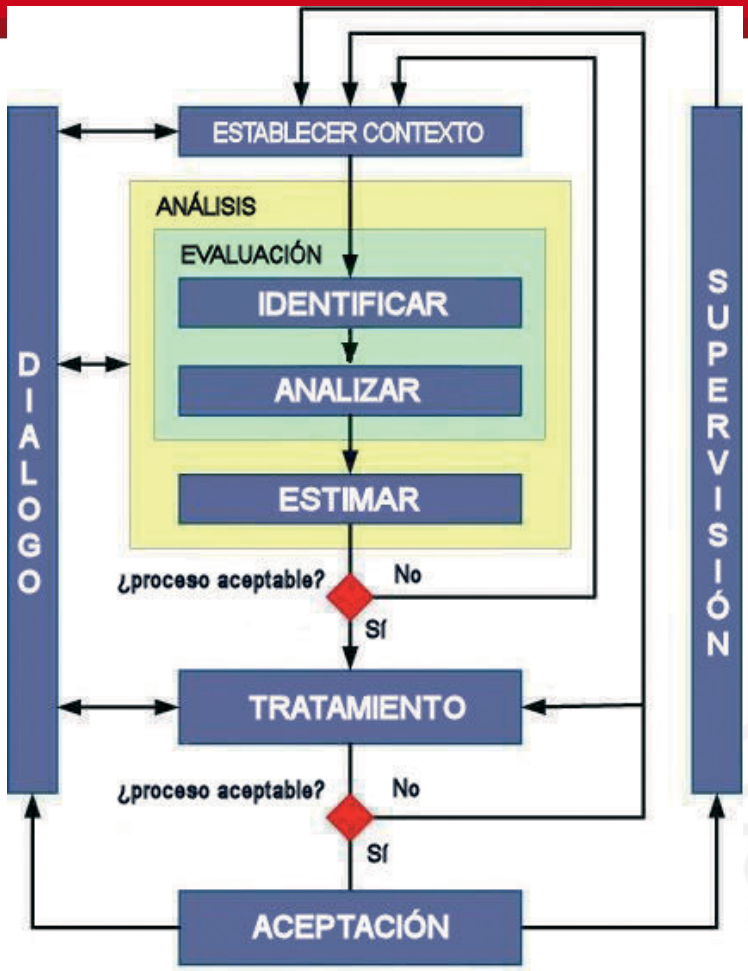

Figura 4. Metodología AS/NZS 4360 [3]

Las etapas para evaluar el riesgo con la metodología AS/NZS 4360 se pueden apreciar en la Figura 5.

- **Establecer el contexto:** Se refiere a definir el marco estratégico, organizacional y de gestión de riesgo. Se definen los criterios a tomar para la evaluación del riesgo y la estructura a utilizar para categorizar los riesgos.

- **Identificación de riesgos:** En esta etapa se realiza un análisis de lo que puede suceder, cómo puede suceder y las herramientas a utilizar y técnicas a utilizar para la identificación de los riesgos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

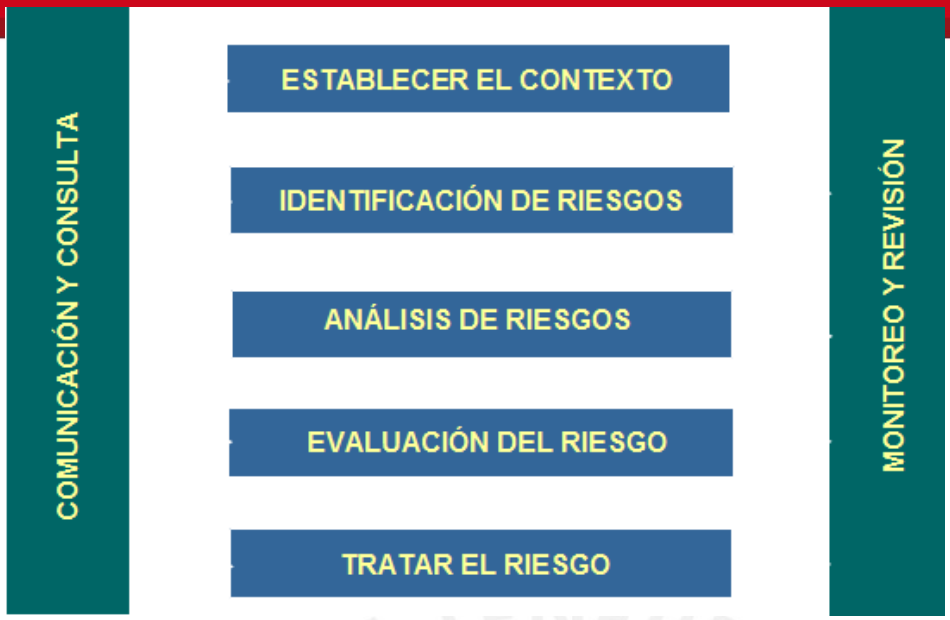

Figura 5. Etapas de AS/NZS 4360 [3]

- **Análisis de riesgos:** Se definen las herramientas y técnicas para el análisis, se analizan los controles existentes y se define el tipo de análisis a realizar a los riesgos, que puede ser cuantitativo o cualitativo.

- **Evaluación del riesgo:** Utilizando lo definido anteriormente, se procede a evaluar el riesgo. Involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente. El producto de una evaluación de riesgo es una lista de riesgos con prioridades para una acción posterior. Si los riesgos resultantes caen dentro de las categorías de riesgos bajos o aceptables, pueden ser aceptados con un tratamiento futuro mínimo. Estos deben ser monitoreados y revisados periódicamente. Si no caen en una categoría de riesgos bajos o aceptables, deberían ser tratados utilizando una o más opciones consideradas en el tratamiento de riesgo, que es la siguiente fase. [3]

- **Tratar el riesgo:** Se identifican opciones para el tratamiento de riesgos, que puede ser asumir el riesgo, reducir la posibilidad que ocurra, transferir el riesgo a alguna compañía aseguradora o reducir la

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

consecuencia. Se evalúan las opciones según costo/beneficio, se toma una decisión y se implementa. [3]

- **Monitorear el riesgo:** Se realiza un monitoreo de cada uno de los riesgos identificados para evaluar si los riesgos se están mitigando correctamente y poder analizar si algún riesgo ha cambiado con el tiempo.

- **Comunicar y consultar:** Se encarga de comunicar e involucrar en el proceso de tratamiento de riesgos a aquellas personas que deben ser involucradas.

El proceso de tratamiento de riesgo, visto como un diagrama de flujo, lo podemos apreciar en la figura 6.

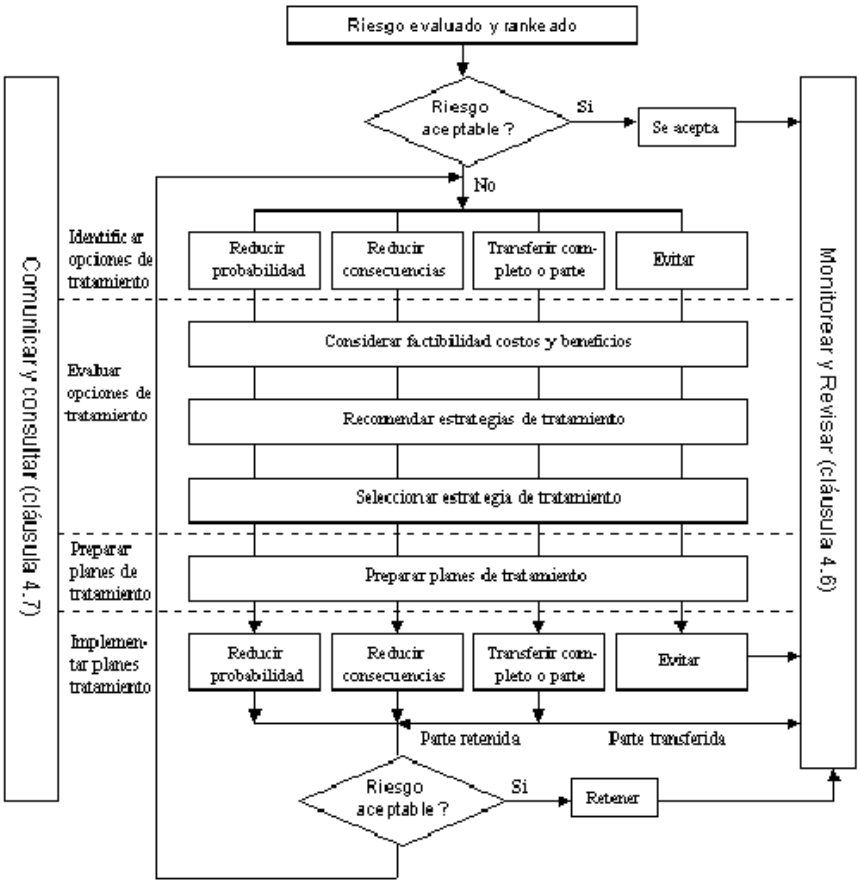

Figura 6. Proceso de Tratamiento de Riesgo [3]

Tesis publicada con autorización del autor
No olvide citar esta tesis

1.3.3. MAGERIT II

MAGERIT[10], desarrollada en España por el Consejo Superior de Administración Electrónica es, al igual que AS/NZS, una metodología para administrar riesgos, que persigue los siguientes objetivos:

- Hacer saber a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de mitigarlos a tiempo
- Ofrecer un método para analizar los riesgos
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control
- Apoyar la preparación a la empresa para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso

El análisis de riesgos propuesto por MAGERIT II es una aproximación metódica que permite determinar el riesgo siguiendo los siguientes pasos:

- Determinar los activos relevantes para la empresa
- Determinar las amenazas a la que están expuestos aquellos activos
- Estimar el impacto, definido como el daño sobre el activo, si se llega a concretar la amenaza
- Valorar dichos activos en función del coste que supondría para la empresa recuperarse ante un problema de disponibilidad, integridad o confidencialidad de información
- Valorar las amenazas potenciales
- Estimar el riesgo

Magerit cuenta con una herramienta de gestión de Análisis de Riesgos EAR/PILAR y el tipo de reporte es Cuantitativo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

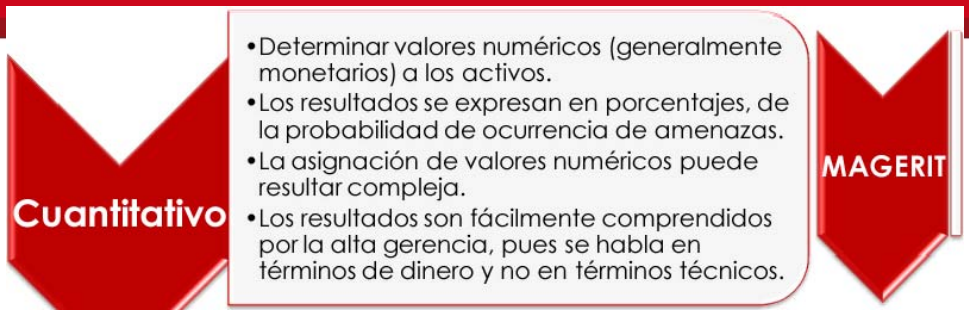

Figura 7. Magerit como metodología de tipo cuantitativo [10]

1.3.4. ISO/IEC 27001:2005 [2]

Publicada el 15 de Octubre de 2005, es la norma principal de la familia de la ISO27000, y contiene los requisitos básicos que debe tener todo sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma sobre la cual se certifican, por auditores externos, los SGSI de las organizaciones. A pesar de no ser obligatoria la implementación de todos los controles, se debe argumentar la no aplicabilidad de los controles no implementados. Recomienda el uso del ciclo Plan – Do – Check – Act para el diseño de un SGSI.

1.3.5. ISO/IEC 27002 :2005 [2]

Describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, mencionados en el anexo A de la ISO 27001, 39 objetivos de control y 133 controles.
Los dominios a tratar son los siguientes:

- **Políticas de Seguridad:** Busca establecer reglas para proporcionar la dirección gerencial y el soporte para la seguridad de la información. Es la base del SGSI.

- **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.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- **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.

- **Seguridad de los 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.

- **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.

- **Gestión de comunicaciones y operaciones:** Esta sección busca asegurar la operación correcta de los equipos, así como la seguridad cuando la información se transfiere a través de las redes, previniendo la pérdida, modificación o el uso erróneo de la información.

- **Control 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.

- **Sistemas de información, adquisición, desarrollo y mantenimiento:** 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.

- **Gestión de incidentes de seguridad de la 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

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

básicamente definir de forma clara pasos, acciones, responsabilidades, funciones y medidas correctas.

- **Gestión de 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 empresa cumpla 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.

1.3.6. Circular G140-2009-SBS

La circular G-140-2009-SBS, elaborada en abril del 2009 por la Superintendencia de Banca y Seguros, obliga a las entidades financieras que son reguladas por este organismo a establecer, mantener y documentar un Sistema de Gestión de Seguridad de la Información (SGSI) tomando como referencia la ISO 17799 e ISO 27001. El objetivo de implementar el SGSI es de brindar seguridad a los activos de información más importantes como resultado del análisis de riesgo y sobre todo cumpliendo con las expectativas de todos los interesados del sistema, clientes, comunidad, estado, proveedores, y la misma entidad financiera entre otros. Los controles con los que cuenta la circular, especificados en el artículo 5º, son los siguientes:

- Seguridad lógica
- Seguridad de personal
- Seguridad física y ambiental
- Inventario de activos y clasificación de la información
- Administración de las operaciones y comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas informáticos
- Procedimientos de respaldo
- Gestión de incidentes de seguridad de información.
- Cumplimiento normativo

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Privacidad de información

1.3.7. Análisis de Impacto en el Negocio (BIA)

El BIA [12] es un informe gerencial el cual ofrece los siguientes resultados:

- Mide el impacto tangible e intangible de una interrupción.
- Determina la criticidad de los procesos de negocio, funciones, departamentos y áreas de trabajo y su relación con la función total organizacional.
- Determina el tiempo crítico de las aplicaciones, sistemas, data y telecomunicaciones para las funciones de negocio.

A través de este informe se determina y se justifica la inversión en las estrategias de continuidad que sean necesarias para la empresa. Para poder definir el alcance de un SGSI de manera adecuada se requiere, en primer lugar, determinar el impacto que una interrupción de los servicios de TI pueden tener en el negocio.

Uno de los supuestos básicos sobre los cuales se fundamenta el análisis de impacto es que cada componente de la organización depende de la continuidad de los otros componentes, pero algunos son más críticos que otros y requieren mayor asignación de recursos en el momento de un desastre.

El objetivo de un análisis de impacto es conocer la relación entre la tecnología existente, los servicios ofrecidos por el departamento de TI y los procesos de negocio que los utilizan. Permite abordar un plan de acción con sólidos elementos de criterio basados no sólo en necesidades de capacidad, sino también de seguridad.

Para poder definir las contingencias deseadas es necesario conocer los servicios de TI que el departamento de informática ofrece a la compañía, sus vulnerabilidades, así como las amenazas y posibles impactos; además de identificar qué servicios de TI soportan los procesos de negocio de la compañía.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Los servicios de TI han de ser analizados en función de diversos parámetros:

- Consecuencias de la interrupción del servicio en el negocio:
  - Pérdida de rentabilidad.
  - Pérdida de cuota de mercado.
  - Mala imagen de marca.
  - Otros efectos secundarios.
- Cuánto se puede esperar a restaurar el servicio sin que tenga un alto impacto en los procesos de negocio.

Dependiendo de estos factores se buscará un balance entre las actividades de prevención y recuperación teniendo en cuenta sus respectivos costes financieros. [12]

1.4. Métodos y Procedimientos

Tomando como referencia lo especificado en la norma ISO 27001, en la sección 4.2.1 Establecer el SGSI, se define la siguiente metodología con el objetivo de desarrollar el proyecto de tesis, utilizando las metodologías, marcos de control y buenas prácticas mencionadas en los puntos anteriores:

1. Identificar los procesos “core” de negocio, con los que opera normalmente una compañía de seguros en general.
2. Realizar un análisis de impacto del negocio, a los procesos identificados, para definir el alcance del SGSI y definir sobre qué procesos trabajar.
3. Evaluar la metodología de análisis de riesgo a utilizar para analizar los procesos de negocio.
4. Realizar un análisis de riesgo en cada uno de los procesos identificados, utilizando la metodología escogida en el punto 3.
5. Definir los controles que se ajusten a los procesos identificados, según la plataforma de control Cobit [4], complementando con los controles de la ISO/IE 27002:2005 [5].
6. Definir una política de seguridad, apoyada en normas, estándares y procedimientos, que den un sustento a los controles seleccionados para cubrir la problemática.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

2. Identificación de procesos y análisis de impacto de negocio

Según lo expuesto en el capitulo anterior, el primer paso para poder desarrollar un SGSI es delimitar un alcance. Para ello, se debe identificar que procesos de la compañía son considerados principales, identificando primero todos los procesos con los que cuenta la empresa para luego, con ayuda de un análisis de impacto de negocio, poder identificar los procesos considerados como “core” y delimitar el SGSI en base a ellos. Posteriormente conforme se vaya madurando el SGSI y según las evaluaciones respectivas, se debe ir ampliando el alcance hasta abarcar todos los procesos de la empresa.

2.1. Identificación de procesos

Un proceso es un conjunto de tareas lógicamente relacionadas que existen para conseguir un resultado bien definido dentro de un negocio; por lo tanto, toman una entrada y le agregan valor para producir una salida. Los procesos tienen entonces clientes que pueden ser internos o externos, los cuales reciben a la salida, lo que puede ser un producto físico o un servicio. Estos establecen las condiciones de satisfacción o declaran que el producto o servicio es aceptable o no. [16]

Tesis publicada con autorización del autor
No olvide citar esta tesis

Para proceder a identificar, tanto los procesos core del negocio, como los procesos operativos y de soporte, se tuvo que realizar un proceso de levantamiento de información, y adaptar la información adquirida para poder amoldar estos procesos para una compañía de seguros en general. Cabe resaltar que, según el enfoque estratégico de la compañía, va a variar la distribución de los procesos, ya que éstos se van a enfocar en lo que la compañía considere le va a dar mayor valor.

A continuación, se describirán algunos de los procesos que soportan las distintas líneas de producto de las compañías de seguro. Las líneas de producto no se están considerando, ya que el hecho que un producto se desarrolle o no va a depender de cada compañía.

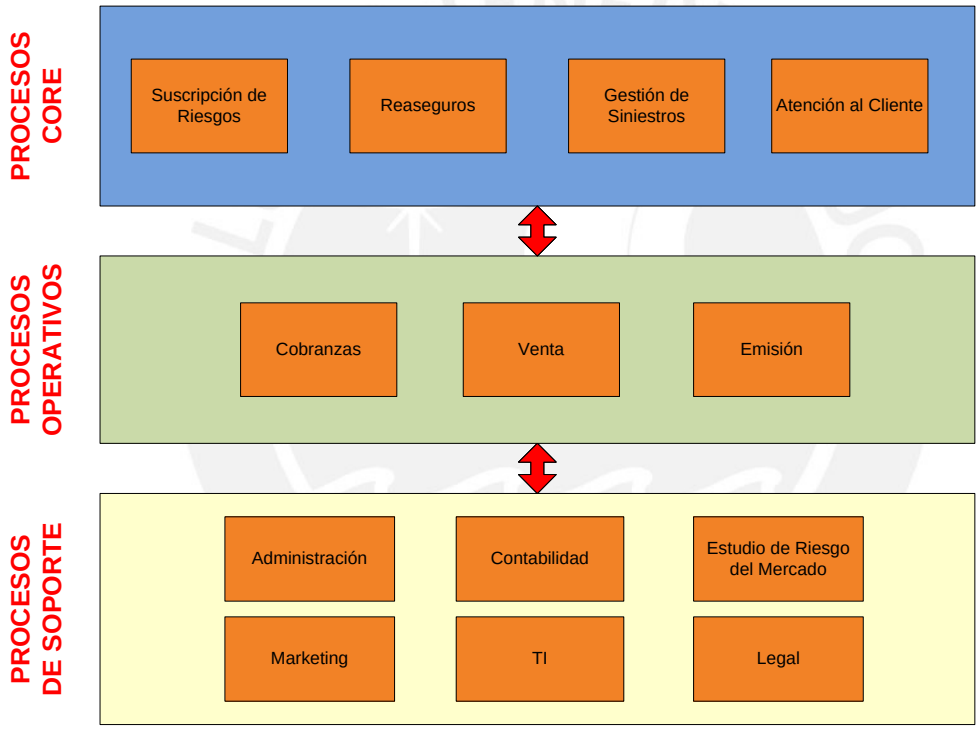

Figura 8. Mapa de procesos

2.1.1. Procesos Core

Los procesos core son aquellos procesos que dan valor al cliente, es decir, que son la parte principal del negocio. Son procesos que si no existieran, la

Tesis publicada con autorización del autor
No olvide citar esta tesis

compañía no podría funcionar como es debido. Entre los procesos “core” identificados se tienen los siguientes:

2.1.1.1. Reaseguros

El proceso puede iniciar de 4 formas:

- Reaseguro automático
- Reaseguro aceptado
- Fronting
- Reaseguro facultativo

Luego se procede a la administración de las notas de crédito y débito, en el que se reciben las notas de crédito o débito y se pagan las primas a los reaseguradores. Se procede al cierre del reaseguro, en el que se comunica la fecha límite para cierre por áreas y se genera el archivo de asiento definitivo para las primas.

Con esta información, se procede a la contabilización, donde se generan las cuentas corrientes, y se da una contabilización general y se generan algunos reportes de importancia. Para la generación de los reportes, se recopilan los datos y se elaboran los reportes para las entidades reguladoras, como la SBS, o para informes o controles internos que pueda realizar auditoría.

2.1.1.2. Siniestros.

El proceso se inicia cuando se comunica la ocurrencia del siniestro. Para esto, el asegurado informa sobre la ocurrencia del siniestro. Se asigna el caso a atender y se envía a un representante al lugar del siniestro, mientras que se procede a registrar la información.

Luego se procede a evaluar el caso, y se gestionan los pasos necesarios a seguir para llegar a una solución (estos pasos van a depender del proceso de cada empresa y del tipo de producto). Los resultados de la evaluación se envían y, en caso sea válido, se procede a la aprobación del presupuesto. En caso no sea válido, se le comunica al cliente las razones del rechazo. En este caso, el cliente puede realizar un reclamo por parte por diferentes medios

Tesis publicada con autorización del autor
No olvide citar esta tesis

(estos medios van a depender de los canales de atención con que cuente al empresa), el cual se registra y se procede a elaborar una carta de respuesta al cliente para informarle los motivos que justifican la resolución dada.

2.1.1.3. Suscripción de Riesgos.

El proceso de suscripción de riesgos normalmente viene ligado al proceso de Venta y Emisión, por lo que se describirá el flujo que sigue el proceso de VSE (venta, suscripción y emisión).

El proceso inicia con la venta y suscripción de una póliza nueva. En ese caso, se recibe la cotización del cliente o del corredor, y se define la calidad de riesgo. Una vez que se evalúa la situación, se puede confirmar la cuenta ganada o bien se rechaza la propuesta de cotización y solicita una emisión al respecto. El proceso también puede empezar por medio de un concurso público o adjudicación directa de entidades del estado. Para esto, se compran las bases por el SEACE y se presenta la propuesta en la convocatoria. Si la propuesta presentada es buena, se suscribe el contrato. En caso contrario, se pierde la convocatoria.

Si se confirma la venta, se procede a revisar las cuentas en conflicto, en caso hayan. Se registra una cuenta en el sistema de prospectos que ya ha sido registrada anteriormente, lo cual crea un conflicto. Se resuelve el conflicto y se procede a efectuar la venta.

Posteriormente, pasa al proceso de emisión, en el que se recibe la solicitud con datos del cliente y datos del riesgo a emitir y se emite la póliza, se imprime y se envía a un compaginador. Para esto, debe haber pasado por el proceso de gestión facultativa, en el que se recibe la información para preparar el esquema de reaseguro final, y este esquema se ingresa a emisión.

Mientras se tarda el proceso, el cliente puede solicitar a la empresa para que emita una cobertura provisional de siniestros. Esta solicitud se aprueba o desaprueba, y en caso se apruebe, se emite una cobertura provisional mientras se formaliza el proceso de emisión de la póliza. Cuando el proceso de emisión de la póliza se termina, se da el proceso de compaginación y despacho. Para

Tesis publicada con autorización del autor
No olvide citar esta tesis

esto, las pólizas debidamente autorizadas son enviadas a un despacho, y al cliente.

Cuando se desea modificar las condiciones del contrato otorgado, ya sea para ampliar o restringir la cobertura, se realiza el proceso de endosos. Para esto, se recibe una solicitud de endoso de póliza, y se emite el endoso durante la vigencia de la póliza para modificar o corregir el contrato otorgado.

Cuando una póliza está por vencer, se genera un proceso de renovación. Para esto, se genera una relación de pólizas a renovar automáticamente o una propuesta de renovación y se valida con el cliente si desea seguir afiliado o no. Posteriormente, se renueva la póliza automáticamente y/o con nuevas condiciones.

2.1.1.4. Atención al Cliente.

En este proceso, se ven las distintas maneras como se puede atender al cliente. La atención se puede iniciar, ya sea por teléfono, por alguno de los canales con los que cuente la empresa para atender al cliente o de manera personal. De la forma como requiera atención el cliente, siempre va a ser atendido, ya sea por un operador (en el caso de llamadas u otro canal de atenciòn) quien atenderá al usuario o por un anfitrión, quien va a consultar al cliente sobre la transacción que desea realizar, y posteriormente sacará el boleto de atención y le indicará hacia dónde debe dirigirse.

2.1.2. Procesos Operativos

Entre los procesos operativos identificados, se encuentra el proceso de cobranzas, el proceso de ventas y el proceso de emisión, pero los dos últimos van de la mano con el proceso de Riesgos, por lo que han sido mencionados anteriormente.

2.1.2.1. Cobranzas.

El proceso inicia con una solicitud de financiación. Después de un proceso de emisión, las pólizas pueden haber sido gestionadas con financiamiento a un determinado plazo, o quizás a una sola cuota. Luego el cliente solicita una

Tesis publicada con autorización del autor
No olvide citar esta tesis

financiación o reprogramar las cuotas pendientes, para lo cual el personal de Cobranzas valida si la financiación se encuentra dentro de las políticas del área financiera para proceder a la misma, o solicitar las autorizaciones respectivas.

En esta etapa se financia la póliza o se rechaza. En caso se acepte la póliza, se ingresa en el sistema. Posteriormente, se da inicio al proceso de gestión de cobranzas, en el que se revisa a cada uno de los clientes y pasa a una fase de anulación o rehabilitación de pólizas. A aquellos clientes que califican para la anulación por falta de pago, se le anulan las pólizas. Si se da el caso que una póliza anulada ha sido pagada por el cliente se procede a la habilitación, que consiste en marcar la póliza y emitir un nuevo documento.

Luego pasa a una etapa de recaudación, que es un servicio que se realiza en el área luego de obtener la información de pagos, o documentos que acrediten pago por alguna vía y se registran en el sistema. Posteriormente se da el proceso de comisiones, que es un servicio que se brinda a agentes y canales en el cual se calcula, modifica, adelanta comisiones y se realiza el pago de los bonos, así como también la anulación o la rehabilitación de las cuentas. Para esto, se reciben las facturas del agente y se verifican. Cuando pasan el proceso de verificación, se procede al pago de las comisiones. En base a las pólizas con morosidad determinadas por la SBS se aprovisiona, se generan los reportes y se calcula a través de SUCAVE (Submódulo de Captura y Validación Externa), que es un software aplicable a las empresas del Sistema Financiero [19].

2.1.3. Procesos de Soporte

De los procesos de soporte se describirá el proceso de TI, por ser el proceso que participa en todos los procesos de la compañía.

2.1.3.1. Soporte de TI.

Dentro de lo que corresponde a soporte de TI, CobiT menciona que existen 34 procesos en toda área de TI. En este segmento se van a mencionar 4 procesos que se cumplen en la mayoría de empresas: la planificación, el desarrollo, soporte a usuarios y compras y contratación.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Para la planificación, se revisan los lineamientos de la compañía, y cómo afectan estos al área. Se revisan los requerimientos y se realiza un costeo de los mismos, para crear un presupuesto. Luego se aprueba el presupuesto, para el próximo periodo según el plan estratégico de la compañía. Posteriormente, de manera periódica, se tienen reuniones para priorizar los requerimientos y acordar las fechas de inicio de las atenciones. Por último, se definen los indicadores de desempeño y operativos, para enviar las tareas a los responsables.

Para el desarrollo, primero se tienen que evaluar los requerimientos de la unidad. Una vez que se han acordado los requerimientos, se procede al diseño de la aplicación. Posteriormente sigue una etapa de certificación, en la que se realiza el control de calidad de la aplicación y pruebas del sistema, en un ambiente controlado similar al ambiente de producción (normalmente llamado ambiente de pre-producción o de pruebas). De esta etapa no sale hasta que se corrigen los errores que son encontrados por los usuarios que certifican la aplicación. También se puede realizar un proceso de auditoría sobre las pruebas que se han realizado a la aplicación. Una vez que sale de la etapa de certificación, se tiene que anunciar su pase a producción. Esto sólo se realiza cuando se tiene la certeza que la aplicación funciona correctamente.

Con relación al proceso de soporte a usuarios, cuando un usuario tiene un problema con alguna aplicación, equipo, entre otros, o simplemente desea algo adicional, que puede ser un acceso, un cambio de equipo, entre otros, realiza un requerimiento de atención a través de Help Desk, quien se encarga de atender el pedido, recoger la información, solicitar la autorización respectiva y remitir la atención a la unidad que corresponde. Una vez realizada la atención, se encarga de informarle al usuario y se le pide su conformidad. Si no hay problemas, se procede a cerrar el requerimiento. En caso el usuario detecte algún problema en la atención, le informa a Help Desk, quienes abren la solicitud y la vuelven a remitir a la unidad respectiva para su atención.

Para el caso de compras y contratación, básicamente se realiza la compra o contratación de plataforma, donde se realiza la solicitud de compra o contratación de servicios, y se envía la orden de compra al proveedor que se seleccione, previa evaluación. Para el caso de la compra o contratación de servicios, en lo que a sistemas se refiere, se realiza la solicitud de contratación

Tesis publicada con autorización del autor
No olvide citar esta tesis

de personal y se gestiona el requerimiento con el proveedor seleccionado. Para ambos casos, se manejan las facturas respectivas, donde el proveedor envía la factura al jefe del área y se envía la factura con un sustento al área encargada de realizar los pagos. Los montos deben estar dentro de lo presupuestado en la etapa de planificación.

2.2. Análisis de impacto de negocio - Business Impact Analysis (BIA)

En la actualidad casi todas las empresas, grandes y pequeñas, dependen en mayor o menor medida de los servicios informáticos, por lo que cabe esperar que una falla de los servicios de TI afecte a, prácticamente, todos los aspectos del negocio. Sin embargo, es evidente que hay servicios TI estratégicos de cuya continuidad puede depender la supervivencia del negocio y otros que aumentan la productividad de la fuerza comercial y de trabajo. [12]

El BIA indica qué procesos o áreas del negocio son las más críticas, qué aplicaciones se deben llevar a un centro de cómputo remoto, por ejemplo, para procesar información el día que ocurra una catástrofe, entre otras cosas. Sin conocer los riesgos reales a los que se enfrenta la infraestructura de TI es imposible definir el alcance del SGSI, ya que para esto se necesita definir los procesos importantes sobre los cuales se va a diseñar el sistema. Se debe enumerar y evaluar, dependiendo de su probabilidad e impacto, los diferentes factores de riesgo. Para ello se debe:

- Conocer en profundidad la infraestructura TI y cuáles son los elementos de configuración involucrados en la prestación de cada servicio, especialmente para cada uno de los procesos críticos y estratégicos.
- Analizar las posibles amenazas y estimar la probabilidad de ocurrencia.

Gracias a los resultados de este análisis se dispondrá de información suficiente para definir el alcance del sistema, proponer diferentes medidas de prevención y recuperación que se adapten a las necesidades reales del negocio. La prevención frente a riesgos genéricos y poco probables puede ser muy cara y no estar siempre justificada. Sin embargo, las medidas preventivas o de recuperación frente a riesgos específicos pueden resultar sencillas, de rápida implementación y relativamente baratas.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Generalmente el informe BIA está compuesto por dos bloques, uno gerencial y uno de soporte. El bloque de soporte tiene como objetivo dejar constancia en detalle de los resultados en un informe gerencial, en caso fuera cuestionado. Para fines prácticos, en la tesis se mostrará el bloque de soporte que viene a ser el detalle del BIA propiamente dicho. Adicionalmente, el BIA determina el RTO y el RPO. Para determinar el RTO, se toma en cuenta la criticidad del proceso. Si el riesgo afecta a algún proceso core o un proceso que lo soporte, el RTO deberá ser menor a comparación de los demás procesos de la compañía.

- RTO: Son las siglas de Recovery Time Objective. Es el máximo tiempo permitido que un proceso puede estar caído como consecuencia de un evento catastrófico, antes de un colapso.
- RPO: Son las siglas de Recovery Point Objective. Son los primeros datos que permiten volver a ofrecer el servicio. Hay que identificar si para la recuperación del proceso que se haya visto afectado se puede disponer de información que se tenía en el momento del incidente o si se puede utilizar información anterior (para ésto hay que determinar qué momento, puede ser días, semanas, etc.).

Al momento de realizar el BIA, que se puede apreciar líneas abajo, se han dividido los riesgos en 4 categorías, para poder guardar un orden en la tabulación al momento de presentar el análisis:

- **Riesgos regulatorios:** Se consideran aquellos riesgos asociados a las regulaciones o a posibles cambios regulatorios que pudieran impactar al negocio o al mercado en el corto o el largo plazo.

- **Riesgos reputacionales:** Se consideran aquellos riesgos que tienen un potencial impacto negativo en el valor de la compañía, resultado de un comportamiento por debajo de las expectativas creadas en los distintos grupos de interés: accionistas, clientes, medios, administración, empleados y la sociedad en general.

- **Riesgos operacionales:** Se consideran aquellos riesgos donde las posibles pérdidas directas o indirectas son ocasionadas por procesos

Tesis publicada con autorización del autor
No olvide citar esta tesis

internos inadecuados, fallos tecnológicos, errores humanos o como consecuencia de ciertos sucesos externos que afecten las operaciones de la empresa.

- **Riesgos de negocio:** Se considera cualquier otro de los riesgos no mencionados anteriormente asociados a la continuidad del negocio, incluyendo, por ejemplo: riesgos geológicos, riesgos biológicos, estrategias de los competidores, entre otros.

Para el BIA se definirán los RTO a considerar:

Nivel RTO	Intervalo de Recuperación (en horas)
1	0 – 8
2	8 – 16
3	16 – 24
4	24 – 32
5	32 – 40
6	40 – 48

Tabla 1. Niveles de RTO

A continuación se muestra parte del desarrollo del BIA elaborado para el desarrollo de la tesis, la matriz en su totalidad se puede apreciar en la sección de Anexos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Página dejada en blanco intencionalmente

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANALISIS DE IMPACTO DE NEGOCIO REALIZADO PARA DEFINIR EL ALCANCE DEL SGSI *							
Riesgo	**Procesos afectados**	**Frecuencia de ocurrencia**	**Impacto**	**Prioridad**	**Nivel RTO**	**Recursos afectados ****	**Comentarios**
Riesgos Regulatorios							
Incumplimiento de regulaciones	Legal	Baja	Alto	Media	3	Personas, Sistema de normas.	Como por ejemplo, cumplir con la circular G140
Incumplimiento de normas de reporte y tributarias	Legal, Contabilidad, Cobranzas	Baja	Medio	Media	3	Sistema de Contabilidad, contadores	-
Incumplimiento de contratos	Legal	Baja	Medio	Media	3	Sistema de Legal, equipo de legal	No cumplir los contratos con los clientes y/o empresas.
Riesgos Reputacionales							
Efectos negativos de la opinión pública	Atención al Cliente	Baja	Alto	Media	3	Red, salida a Internet, líneas telefónicas, personas, equipos.	Por publicidad negativa y/o rumores infundados.
Daños en la marca por la falla en la gestión de relaciones públicas.	Atención al Cliente, Marketing	Baja	Alto	Media	4		-

Tesis publicada con autorización del autor
No olvide citar esta tesis

Riesgo	Procesos afectados	Frecuencia de ocurrencia	Impacto	Prioridad	Nivel RTO	Recursos afectados **	Comentarios
Servicio inoportuno y demorado a los clientes.	Atención al Cliente	Baja	Medio	Media	1	Red, salida a Internet, sistemas de información de Siniestros, líneas telefónicas, personas, equipos.	Se puede estimar que, una vez que el cliente presenta la queja, para no perderlo se trata de compensar de alguna manera el mal servicio.
Información entregada a los clientes engañosa o desorientadora	Atención al Cliente, TI	Baja	Medio	Media	1	Red, sistemas de información de Siniestros, sistemas de información de Atención al Cliente, salida a Internet, líneas telefónicas, personas, equipos.	Se puede deber a la inexperiencia del personal de la compañía.
Riesgos Operacionales							
Pérdida o daño de capacidades operativas a causa de problemas con los equipos	Todos	Media	Medio	Media	1	Servidores, red, equipos, aplicaciones.	Es un tiempo máximo estimado de recuperación.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Riesgo	Procesos afectados	Frecuencia de ocurrencia	Impacto	Prioridad	Nivel RTO	Recursos afectados **	Comentarios
Pérdida o daño de capacidades operativas a causa de problemas con las instalaciones	Todos	Baja	Medio	Media	1	Servidores, red, equipos, aplicaciones.	Dependiendo del problema.
Pérdida o daño de capacidades operativas a causa de problemas con los servicios	Todos	Media	Medio	Media	1	Servidores, red, equipos, aplicaciones.	Depende del tiempo que demore el feedback y la corrección del proceso.
Pérdida o daño de capacidades operativas a causa de problemas con los sistemas de información	Todos	Media	Medio	Media	1	Servidores, red, equipos, aplicaciones.	Dependiendo la complejidad del problema en el sistema.
Diseño o desempeño inadecuado de la infraestructura existente de gestión de riesgos	Todos	Media	Alto	Alta	1	Personas, sistema de normas, matriz de riesgos.	-
Problemas por entrega de servicios causados por debilidades en procedimientos de operación	Atención al Cliente, Gestión de Siniestros, VSE, Cobranzas	Media	Medio	Media	1		Depende del tiempo estimado para la revisión periódica de las operaciones.
Riesgo	**Procesos afectados**	**Frecuencia de ocurrencia**	**Impacto**	**Prioridad**	**Nivel RTO**	**Recursos afectados ****	**Comentarios**

Tesis publicada con autorización del autor
No olvide citar esta tesis

Modificación no autorizada de información.	TI, VSE, Reaseguros, Gestión de Siniestros.	Media	Alto	Alta	1	Servidores, red, Sistema de seguridad de aplicaciones	Tiempo máximo para darle solución a esa brecha de seguridad, lo ideal es que se solucione el problema una vez detectada la modificación.
Perdida de disponibilidad de información	Todos	Media	Alto	Alta	1	Servidores, BD de respaldo, red	Tiempo máximo, lo ideal es que dure horas, ya que se debe definir un plan de contingencia para estos casos.
Perdida de disponibilidad de información	Todos	Media	Alto	Alta	1	Servidores, BD de respaldo, red	Tiempo máximo, lo ideal es que dure horas, ya que se debe definir un plan de contingencia para estos casos.
Interrupción del servicio	TI	Baja	Alta	Media	1	Servidores, BD de respaldo, red, equipos, aplicaciones.	Tiempo máximo, lo ideal es que dure horas, ya que se debe definir un plan de contingencia para estos casos.
Problemas por entrega de servicios causados por fallas de controles internos	Atención al Cliente, Gestión de Siniestros, VSE	Media	Medio	Media	1		
Riesgo	**Procesos afectados**	**Frecuencia de ocurrencia**	**Impacto**	**Prioridad**	**Nivel RTO**	**Recursos afectados ****	**Comentarios**

Tesis publicada con autorización del autor
No olvide citar esta tesis

Problemas por entrega de servicios causados por fallas de sistemas de información	Atención al Cliente, Gestión de Siniestros, VSE, TI	Media	Medio	Media	1	Red, sistemas de información de Siniestros, sistemas de información de Atención al Cliente, salida a Internet, líneas telefónicas, personas, equipos.	Tiempo máximo, mientras se genera el ticket de atención y se deriva al área que dará solución al problema,
Problemas por entrega de servicios causados por equivocaciones de usuarios	Atención al Cliente, Gestión de Siniestros, VSE, Cobranzas	Media	Medio	Media	1		Depende del tiempo estimado para la revisión periódica de las operaciones. En todo caso, la modificación del trato con el cliente ya no se puede realizar, pero se puede ajustar los controles para que no vuelva a suceder.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

3. Análisis y tratamiento de riesgos

Para proceder a realizar el análisis y el tratamiento de riesgos, debemos definir el alcance del SGSI. Para esto, se tomarán en consideración aquellos riesgos cuyo RTO sea menor, y que se repitan de manera considerable. Al realizar el análisis sobre el BIA, se puede apreciar que los procesos a considerar como procesos core son: TI, Atención al Cliente, VSE, Gestión de Siniestros, Reaseguros y Cobranzas. Es sobre estos procesos donde se pondrá un mayor énfasis al momento del análisis de los riesgos y en la definición de controles para garantizar un nivel aceptable de seguridad en la empresa. Luego de haber definido el alcance del sistema, tras haber identificado los procesos importantes para una compañía de seguros, se procede a analizar el flujo de cada uno de los procesos, de una manera más detallada, y se identifican las vulnerabilidades que se pueden encontrar dentro del flujo del proceso.

La metodología escogida para el análisis y tratamiento de riesgos es la metodología AS/NZS 4360 [3] , la cual se explica en las siguientes líneas.

Tesis publicada con autorización del autor
No olvide citar esta tesis

3.1. Establecer el contexto

Establecer el contexto es el primer paso en la metodología AS/NZS 4360 para administración de riesgos. El análisis del entorno permite definir los parámetros para que los riesgos puedan ser gestionados, es decir que, para reconocer un riesgo, es necesario conocer qué es un riesgo para la organización. El contexto define el alcance para el proceso de administración de riesgos. Incluye la estrategia a tomar, la organización de la empresa y las consideraciones de los riesgos que puede tomar la compañía.

El contexto estratégico define la relación entre la organización y el entorno. Los factores a considerar que influyen en esta relación son factores financieros, operacionales, de competencia, políticos, sociales, orientados al cliente, culturales y legales.

El contexto organizacional provee un entendimiento de la organización, su capacidad y las metas, objetivos y estrategias de la empresa. El tratamiento de los riesgos va a estar estrechamente ligado al plan estratégico de la compañía, ya que conforme la empresa decida innovar sus procesos, van a ir apareciendo nuevos riesgos, y habrá que darle una mayor prioridad a aquellos riesgos que puedan afectar el desarrollo del plan de la compañía, y por ende, que no se cumplan las metas y objetivos trazados. Este contexto es importante porque:

- La administración de riesgos básicamente dentro del contexto busca procurar llevar a cabo las metas y objetivos.
- Si se falla en llevar a cabo los objetivos se dan riesgos que necesitan ser administrados.
- Las metas y estrategias que defina la empresa van a ayudar a definir si el riesgo es aceptable o no.

El contexto de administración de riesgos define en qué parte de la organización (ya sean metas, objetivos o proyectos) se debe enfocar más el proceso de administración de riesgos.

Para asegurar que todos los riesgos significativos se han capturado, es necesario conocer los objetivos de la empresa dentro de los cuales los riesgos son manejados. Un objetivo puede ajustarse según lo que un stakeholder

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

puede decir sobre las operaciones importantes. Si se definen objetivos sin referencias de personas con influencias sobre las operaciones de la empresa, es probable que los problemas que se omitan salgan a la luz en un punto dado, dando a entender que no se ha hecho un buen trabajo en el proceso de administración de riesgos. Un buen criterio es usado para medir el impacto de todo aquello logro que pueda arriesgar el logro de los objetivos. Para que el criterio sea efectivo, debe:

- Ser conciso, es decir, proveer el menor número de medidas que permita cubrir el mayor número de impactos significativos.
- Cubrir todos los aspectos de ocurrencia, lo que significa que se hayan medido todos los impactos significativos.
- Definir las medidas a tomar, y si estas serán en términos cualitativos o cuantitativos.
- Separar el impacto del riesgo de la probabilidad de ocurrencia.

El criterio debe estar orientado hacia una preferencia sobre la dirección en la que se maneja la empresa. [3]

3.2. Identificación de riesgos

En esta etapa, se identifican los riesgos más probables que puedan afectar a los procesos definidos, junto con el impacto que trae consigo cada riesgo y las fuentes que los originan. Es importante ser cuidadoso con la identificación de las fuentes y el impacto, ya que las estrategias a tomar para tratar estos riesgos se darán ya sea de forma preventiva o de forma reactiva.

En un esfuerzo por simplificar la tarea de identificar los riesgos, a veces se cae en el error de no profundizar sobre los distintos riesgos que se pueden presentar y se utiliza una lista de riesgos estándar que normalmente son conocidos y recopilados para prevenir los riesgos en un contexto particular. Un listado de riesgos puede ser fácil de usar y muy práctico, pero bloquea la identificación de riesgos que puede ir más allá de la experiencia que se puede hallar en esa lista.

La mejor forma de identificar riesgos es realizar una lluvia de ideas en un taller de grupo o en un comité formado por gente con bastante experiencia dentro de la compañía y que conozcan muy bien los procesos. La lluvia de ideas nos va a

Tesis publicada con autorización del autor
No olvide citar esta tesis

permitir reducir la probabilidad que no se le preste la suficiente atención a nuevos riesgos que se encuentran emergiendo, y que podríamos obviar usando la técnica del listado de riesgos. Siempre la experiencia y el conocimiento de una persona sobre un proceso en especial, va a ser un aporte valioso en el proceso de la identificación de riesgos. La forma en la que el proceso es administrado puede asegurar que la información histórica no bloquee una evaluación creativa en el futuro, donde los riesgos que nunca se detectaron o nunca aparecieron puedan aflorar, y que los riesgos que en su momento eran familiares disminuyan de manera considerable. [3]

3.3. Análisis de riesgos

En la etapa del análisis de riesgos, identifican los controles que se encuentren implementados actualmente en la compañía que traten los riesgos identificados y evaluar su efectividad. Para este caso, en vista que se está diseñando el sistema, se asume que no hay controles implementados en la compañía y se procederá a diseñar los controles posteriormente. En la etapa de análisis, se asigna a cada riesgo una clasificación significativa, tomando en cuenta factores existentes, los cuales se van a manejar para controlar el caso. A su vez, en esta etapa se analizan los riesgos en términos de probabilidades y consecuencias, así como el nivel de riesgo actual, que resulta producto de una combinación entre la probabilidad y la consecuencia. Para poder utilizar un análisis de impacto cuantitativo es necesario utilizar variables e información con la que no se cuenta actualmente, como por ejemplo, data histórica, valor de los activos, entre otros, por lo que se va a realizar un análisis cualitativo y nos ayudará para las etapas siguientes del proceso de análisis y tratamiento de riesgos. [3]

3.4. Evaluación del riesgo

En la etapa de evaluación del riesgo, se determina si los riesgos son aceptables o no. Esta decisión debe ser tomada por una persona dentro de la compañía con la suficiente autoridad y conocimiento del proceso. En este caso, se recomienda que sean los propietarios de información o gerentes de área los que determinen si el riesgo es aceptable o no. [3]

Si se determina que el riesgo es aceptable, se debe monitorear el riesgo y en caso el riesgo no sea aceptable, debe ser tratado. Para todos los casos, se

Tesis publicada con autorización del autor
No olvide citar esta tesis

debe documentar la evaluación que se ha hecho a cada riesgo, y sustentar el por qué se considera un riesgo aceptable o no. Esto va a permitir poder tomar decisiones en un futuro, ya que puede dar ideas sobre cómo tratar un nuevo riesgo, así como poder revisar los argumentos en caso un riesgo se materialice y haya tenido un impacto mayor al considerado y tomar medidas al respecto.

La evaluación toma el análisis de la etapa anterior y lo revisa, tomando en cuenta las prioridades y requerimientos de la empresa.

3.5. Tratar el riesgo

Esta etapa consiste básicamente en determinar qué se va a hacer en respuesta al riesgo identificado. Para poder tratar un riesgo, hay diferentes estrategias que se pueden tomar:

- Evitar el riesgo.
- Reducir la probabilidad de ocurrencia.
- Reducir la consecuencia después que se materialice el riesgo.
- Transferir el riesgo
- Aceptar el riesgo

La selección de la estrategia a tomar tiene que ver con factores como el costo y la efectividad. El tratamiento de riesgos puede alterar el plan base de la organización. Cualquier plan que se encuentre definido en la empresa antes de que el proceso de tratamiento de riesgos empiece, puede ser aumentado con medidas para tratar los riesgos antes que afloren los riesgos y con planes de contingencia para recuperarse si un riesgo llegara a ocurrir. Ocasionalmente, la mejor manera de tratar un riesgo puede ser adoptar una estrategia alternativa ya sea para evitar el riesgo o, en caso se materialice el riesgo, hacer a la organización menos vulnerable a sus consecuencias.

Luego de la selección de la estrategia, se debe documentar las razones por las cuales se ha tomado esa medida e incluir los detalles de la implementación de la misma. La intención es reducir el nivel de riesgo a un nivel aceptable. [3]

Tesis publicada con autorización del autor
No olvide citar esta tesis

3.6. Monitorear los riesgos

Luego de haber evaluado los riesgos y definir las acciones a tomar para mitigar estos riesgos, se tiene que pasar por una etapa de monitoreo continuo, para medir la efectividad del control y poder detectar nuevos riesgos o si un riesgo ha pasado de un nivel bajo a un nivel alto. Los cambios en el entorno o el descubrimiento de mejor información pueden hacer que la evaluación original esté desactualizada. En ese caso, no es necesario realizar todo el proceso, sólo es cuestión de actualizar aquellas partes que se ven afectadas directamente.

La frecuencia con la que se va a realizar el monitoreo, va a depender del nivel de riesgo asociado al activo de información, el posible impacto en caso se materialice y el tipo de control que se quiera aplicar, así como el costo de implementación del control.

También se monitorean las operaciones de las etapas anteriores, ya que la ejecución del proceso de tratamiento de riesgos utiliza recursos, y se debe velar para que éstos sean manejados de una manera efectiva, y tratar de reducir costos. [3]

3.7. Comunicar y consultar

Esta etapa se da a todo lo largo del proceso de tratamiento de riesgos, y es un componente importante del proceso. Para poder planear y ejecutar el proceso de tratamiento de riesgos es importante involucrar a aquellas personas que cuentan con experiencia y conocimiento de los procesos importantes de la compañía y mantener informada del desarrollo del proyecto a la alta gerencia, haciéndole comprender sobre la importancia del tratamiento de riesgo, los riesgos identificados y las medidas tomadas para lidiar con ellos. [3]

A continuación se muestra, tanto la matriz de análisis de riesgos 5x5 utilizada para clasificar el nivel de riesgo, y en base a este resultado definir la prioridad del mismo, como la matriz de tratamiento de riesgos que servirá de “materia prima” para el desarrollo del SGSI, delimitando el alcance sólo para aquellos procesos definidos como importantes, dentro del análisis del impacto de negocio.

Tesis publicada con autorización del autor
No olvide citar esta tesis

La matriz de análisis de riesgo 5x5 cuenta con una estructura como la que se muestra a continuación:

5x5	Consecuencia				
Probabilidad	Muy Baja	Baja	Media	Alta	Muy Alta
Muy Alta					
Alta					
Media					
Baja					
Muy Baja					

Figura 9. Matriz de riesgos 5x5

El desarrollo de la matriz se podrá apreciar en las páginas siguientes y en los anexos, en la sección "Matriz de análisis de riesgo 5x5" y, posteriormente, se muestra parte del tratamiento de los riesgos (mayor detalle en la sección "Matriz de tratamiento de riesgos" en los Anexos)

El nivel de riesgo, para la matriz, se tomará de la siguiente manera:

Nivel de Riesgo	Color
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

Tabla 2. Niveles de Riesgo

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Página dejada en blanco intencionalmente

Tesis publicada con autorización del autor
No olvide citar esta tesis

MATRIZ DE ANÀLISIS DE RIESGOS 5x5					
5x5	Impacto				
Probabilidad de Ocurrencia	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Muy Alta					
Alta			• Pérdida o daño de capacidades operativas a causa de problemas con los sistemas de información.	• Modificación no autorizada de información. • Dependencia de personal crítico para la empresa • No reclutar, desarrollar o retener a los empleados que cuenten con habilidades o conocimientos apropiados.	
		• Incumplimiento de las metas estratégicas a largo plazo del negocio • Incapacidad de	• Servicio inoportuno y demorado a los clientes. • Pérdida o daño de capacidades	• Diseño o desempeño inadecuado de la infraestructura existente de gestión de	

Tesis publicada con autorización del autor
No olvide citar esta tesis

Media		planear, gestionar y monitorear el desempeño de proyectos, productos, servicios, procesos, personal y canales de información relacionados con tecnología. • Incapacidad de planear y gestionar los recursos requeridos para un proyecto • Riesgo de selección adversa.	operativas a causa de problemas con los equipos. • Problemas por entrega de servicios causados por fallas de controles internos • Problemas por entrega de servicios causados por equivocaciones de usuarios • Fraude por parte de los clientes en contra de la compañía. • No evaluar adecuadamente las capacidades de los proveedores • Pérdidas	riesgos • Perdida de disponibilidad de información • Problemas por entrega de servicios causados por fallas de sistemas de información. • Ausencia de personal técnico calificado para cubrir plazas de alta criticidad • Uso inapropiado de información • Calidad deficiente de los servicios proporcionados por terceros. • Presentación de información inadecuada, imprecisa, incompleta o	

Tesis publicada con autorización del autor
No olvide citar esta tesis

			financieras	inoportuna para apoyar el proceso de toma de decisiones de la gerencia. • Pérdida de clientes. • Pérdida de confidencialidad de información. • Pérdida de integridad de la información.. • Fuga de información, sabotaje y/ robo de información y otros activos por empleados deshonestos o molestos • Divulgar accidental o intencionalmente información que constituye ventaja	

Tesis publicada con autorización del autor
No olvide citar esta tesis

				competitiva.	
Baja			• Incumplimiento de normas de reporte y tributarias. • Incumplimiento de contratos • Información entregada a los clientes engañosa o desorientadora. • Pérdida o daño de capacidades operativas a causa de problemas con las instalaciones	• Incumplimiento de regulaciones. • Efecto negativo de la opinión pública. • Interrupción del servicio • Asegurar por un valor mayor al debido una póliza. • Asegurar algo fuera de lo presupuestado y que debería ser reasegurado.	
Muy baja			• Amenazas a la salud y seguridad del personal	• Pérdida o daño de información u objetos de valor a causa de fraude, robo, negligencia voluntaria, negligencia grave,	• Pérdida parcial o total de la información a causa de un desastre natural

Tesis publicada con autorización del autor
No olvide citar esta tesis

				vandalismo, sabotaje, extorsión, etc. • Pérdida parcial o total de la información a causa de ataques de terceros.	

Tesis publicada con autorización del autor
No olvide citar esta tesis

Matriz de tratamiento de riesgos

Fuente Origen	Causa	Riesgo asociado	I	C	D	Nivel	Prioridad	Estrategia	Acciones a tomar
Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones			X	3	Media	Evitar el riesgo.	• Crear un programa de Seguridad de la Información para cumplir con la regulación G140.
Personas	Personal no capacitado.	Incumplimiento de normas de reporte y tributarias				3	Media	Evitar el riesgo	• Contar con un equipo legal calificado para que pueda verificar detalladamente las cláusulas de los contratos. • Controles de selección rigurosos y detallados para un puesto específico
Infraestructura	Problemas con la conexión a Internet.	Incumplimiento de normas de reporte y tributarias			X	3	Media	Evitar el riesgo.	• Contar con un doble proveedor del servicio.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Fuente Origen	Causa	Riesgo asociado	I	C	D	Nivel	Prioridad	Estrategia	Acciones a tomar
Personas	Personal no capacitado.	Incumplimiento de contratos			X	3	Media	Evitar el riesgo.	• Contar con un equipo legal calificado para que pueda verificar detalladamente las cláusulas de los contratos.
Sistemas de información	Fallas en el sistema.	Incumplimiento de contratos			X	3	Media	Evitar el riesgo.	• Contar con un sistema que permita revisar los contratos vigentes de la compañía.
Personas	Mala atención por parte de la plataforma debido a personal insatisfecho.	Efectos negativos de la opinión pública				3	Media	Reducir la probabilidad de ocurrencia.	• Realizar feedback con los empleados de manera periódica.
Sistemas de información	Mala atención por parte de la plataforma, debido a errores en el sistema.	Efectos negativos de la opinión pública			X	3	Media	Reducir la probabilidad de ocurrencia.	• Desarrollo de políticas sobre adquisición y elaboración de software.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Fuente Origen	Causa	Riesgo asociado	I	C	D	Nivel	Prioridad	Estrategia	Acciones a tomar
Personas	Falta de competencia por parte del personal.	Servicio inoportuno y demorado a los clientes.				3	Media	Reducir la probabilidad de ocurrencia.	• Capacitaciones periódicas al personal.
Sistemas de información	Mala atención por parte de la plataforma, debido a errores en el sistema.	Servicio inoportuno y demorado a los clientes.			X	3	Media	Reducir la probabilidad de ocurrencia.	• Desarrollo de políticas sobre adquisición y elaboración de software. • Definición de tiempos de atención para la solución de problemas en sistemas para las diferentes áreas, definiendo un menor tiempo para aquellas áreas de cara al público.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Fuente Origen	Causa	Riesgo asociado	I	C	D	Nivel	Prioridad	Estrategia	Acciones a tomar
Empleados	Modificación no autorizada por parte de personal no autorizado.	Información entregada a los clientes engañosa o desorientadora	X	X		3	Media	Reducir la probabilidad de ocurrencia.	• Desarrollar políticas de control de acceso. • Definir a los propietarios de información y que indiquen quienes deben de tener acceso y con que nivel de privilegios.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Fuente Origen	Causa	Riesgo asociado	I	C	D	Nivel	Prioridad	Estrategia	Acciones a tomar
Fuentes externas	Modificación no autorizada por parte de fuentes externas.	Información entregada a los clientes engañosa o desorientadora	X	X		3	Media	Reducir la probabilidad de ocurrencia.	• Contar con un centro de cómputo alterno. • Contar con herramientas de prevención, como un firewall o un IDS, para detectar cuando la red está siendo vulnerada. • El uso de honeypots para poder obtener información sobre el ataque empleado y poder realizar las correcciones respectivas. • Desarrollar políticas de control de acceso. • Definir a los propietarios de información y que indiquen quienes deben de tener acceso y con que nivel de privilegios.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Fuente Origen	Causa	Riesgo asociado	I	C	D	Nivel	Prioridad	Estrategia	Acciones a tomar
Sistemas de Información	Falla en los sistemas de información, por lo que la información puede no ser confiable.	Información entregada a los clientes engañosa o desorientadora	X			3	Media	Reducir la probabilidad de ocurrencia.	• Desarrollo de políticas sobre adquisición y elaboración de software. • Realizar un proceso de certificación adecuado antes de pasar los sistemas a producción.
Empleado	Clima laboral no adecuado	Información entregada a los clientes engañosa o desorientadora	X			3	Media	Reducir la probabilidad de ocurrencia.	• Realizar feedback con los empleados de manera periódica.
Instalaciones	Accidentes laborales por problemas con las instalaciones	Pérdida o daño de capacidades operativas a causa de problemas con las instalaciones			X	3	Media	Reducir la probabilidad de ocurrencia.	• Realizar revisiones periódicas sobre las instalaciones.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

4. Desarrollo del Sistema de Gestión de Seguridad de Información

Para poder desarrollar un SGSI es necesario tomar como base, la ISO27001. Este estándar fue confeccionado para proveer un modelo para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de un SGSI. La decisión por parte de la empresa de adoptar un SGSI es una decisión estratégica, ya que el SGSI está fuertemente ligado a las necesidades y objetivos de la misma,

Como se mencionó en el estado del arte, el estándar adopta un proceso para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI en una organización, es decir, adopta el modelo “Plan – Do – Check – Act”, también conocido como PDCA, el cual es aplicado a toda la estructura de procesos del SGSI.

Tesis publicada con autorización del autor
No olvide citar esta tesis

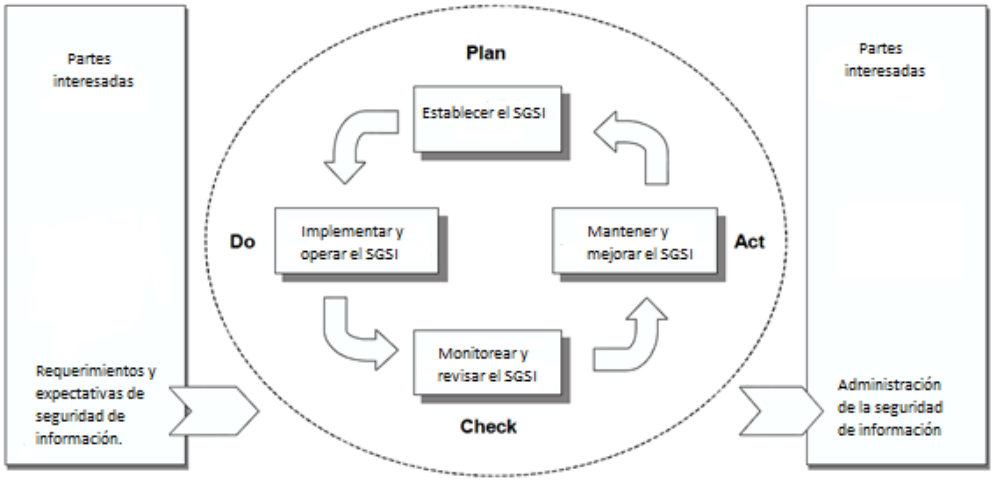

Figura 10. Ciclo PDCA [2]

- **Plan (Establecer el SGSI):** Implica, establecer la política del SGSI, sus objetivos, procesos y procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, con resultados acordes a las políticas y objetivos de toda la organización. El SGSI tiene que ir alineado con el plan estratégico de la compañía.

- **Do (Implementar y operar el SGSI):** Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos que se vayan a definir en la planificación del SGSI.

- **Check (Monitorizar y revisar el SGSI):** Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del SGSI, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.

- **Act (Mantener y mejorar el SGSI):** Realizar las acciones preventivas y correctivas, basados en las auditorías internas y/o externas, revisiones del SGSI o cualquier otra información relevante para permitir la continua mejora del sistema.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Con este método se puede asegurar que un SGSI es dinámico y que se va ajustando a las necesidades de la empresa, según el plan estratégico de la misma y conforme van apareciendo nuevas amenazas y vulnerabilidades.

4.1. Cláusulas de la ISO27001 a considerar para el desarrollo de un SGSI

Los requerimientos que tiene el estándar ISO27001 para un SGSI, son genéricos y aplicables a casi la totalidad de organizaciones. Cuando una organización solicita una conformidad sobre esta norma, hay ciertas cláusulas que son obligatorias y que no se acepta la exclusión de los requerimientos especificados en ellas. Estas cláusulas son:

- SGSI
- Responsabilidades de la Administración
- Auditoría Interna del SGSI
- Administración de las revisiones del SGSI
- Mejoras del SGSI

Cualquier exclusión a los controles detallados por la norma y denominados como necesarios para satisfacer los criterios de aceptación de riesgo, debe ser justificado y se debe poner de manifiesto, o justificar los criterios por los cuales el riesgo es asumido y aceptado. [14]

4.1.1. SGSI

El estándar menciona que la organización debe establecer, implementar, operar, revisar, mantener y mejorar un SGSI que se encuentre debidamente documentado. Es por esta razón que se utiliza el método PDCA. La organización debería tomar en cuenta lo siguiente, al momento de establecer el SGSI:

- Definir el alcance del SGSI teniendo en cuenta las características del negocio, la organización, la locación, los riesgos, la tecnología y la justificación por alguna excepción sobre el alcance.
- Definir una política para el SGSI, considerando las características de la empresa, el negocio, los riesgos, la locación y los procesos tecnológicos. Esto incluye utilizar un framework de control para definir los objetivos de control que servirán de base para el buen desempeño del SGSI.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Definir la metodología de administración de riesgos a utilizar.
- Identificar los riesgos.
- Analizar y evaluar los riesgos
- Evaluar las estrategias a tomar para tratar los riesgos identificados.
- Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.
- Obtener la aprobación de la gerencia sobre el riesgo residual.
- Obtener la aprobación de la gerencia para implementar el SGSI.
- Preparar el documento de aplicabilidad.

Para el caso de esta tesis, se están siguiendo estos pasos. Primero se definió el alcance del SGSI realizando un análisis de impacto de negocio, lo cual permitió identificar los procesos importantes sobre los que se va a enfocar el SGSI, en el capítulo 5. Luego, sobre estos procesos, ya se entró al detalle y se realizó un proceso de administración de riesgos, utilizando el estándar australiano AS/NZS 4360, en el capítulo anterior. Ya durante el desarrollo de este capítulo, y utilizando el tratamiento de riesgos realizado anteriormente, se procederá a identificar los objetivos de control, utilizando el COBIT como la plataforma de control, y mapeando los controles de la ISO27002 que apliquen al caso, para tratar cada uno de los riesgos identificados. Posteriormente, se desarrollará el documento de aplicabilidad para justificar la selección de los controles y la ausencia de otros.

La ISO27001 también indica que los documentos requeridos por el SGSI deben ser protegidos y controlados de alguna manera. Un procedimiento documentado deberá establecer las acciones de administración necesarias para:

- Aprobar documentos y prioridades o clasificación de empleo.
- Revisiones, actualizaciones y reaprobaciones de documentos.
- Asegurar que los cambios y las revisiones de documentos sean identificados.
- Asegurar que las últimas versiones de los documentos aplicables se encuentren disponibles y listas para ser usadas.
- Asegurar que los documentos se encuentren legibles y se puedan identificar fácilmente.
- Asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Asegurar que los documentos de origen externo sean identificados
- Asegurar el control de la distribución de documentos.
- Prevenir el empleo no deseado de documentos obsoletos y aplicar una clara identificación para poder acceder a ellos y que queden almacenados para cualquier propósito.

4.1.2. Responsabilidades de la Administración

El estándar dice básicamente que la administración proveerá evidencias de sus compromisos para el establecimiento, implementación, operación, monitoreo, mantenimiento y mejora del SGSI, teniendo en cuenta:

- Un establecimiento de la política del SGSI.
- Asegurar el establecimiento de los objetivos y planes del SGSI.
- Establecer roles y responsabilidades para la seguridad de la información.
- Comunicar y hacer tomar conciencia a la organización sobre la importancia del SGSI y solicitar el apoyo necesario a los objetivos propuestos por la política de seguridad, sus responsabilidades legales y la necesidad de una mejora continua.
- Proveer suficientes recursos para establecer, operar, implementar, monitorizar, revisar, mantener y mejorar el SGSI.
- Decidir los criterios de aceptación de riesgos y los niveles del mismo.
- Asegurar que las auditorías internas del SGSI sean conducidas y a su vez conduzcan a la gerencia para la revisión del SGSI.

De igual forma, la organización debe asegurar que el personal a quien se le asignen las responsabilidades definidas en el SGSI sea competente y esté en la capacidad de ejecutar las tareas requeridas. Para ello, hay que contar con las herramientas necesarias y una capacitación constante.

4.1.3. Auditoría interna del SGSI

La organización debe realizar auditorías internas al SGSI a intervalos planeados para determinar si los controles, objetivos, procesos y procedimientos continúan conforme al estándar ISO27001 y para analizar y planificar mejoras al sistema. De más está decir que una persona no puede auditar su propio trabajo, ni cualquier otra persona que guarde relación con él.

Tesis publicada con autorización del autor
No olvide citar esta tesis

La responsabilidad y requerimientos para el planeamiento y la conducción de las actividades de auditoría, los informes resultantes y el mantenimiento de los registros serán definidos en un procedimiento

4.1.4. Administración de las revisiones del SGSI

El estándar especifica que las revisiones mencionadas en el punto anterior deberán llevarse a cabo al menos una vez al año para asegurar la vigencia, adecuación y efectividad. Estas revisiones incluirán valoración de oportunidades para mejorar o cambiar el SGSI incluyendo la política de seguridad de información y sus objetivos. Los resultados deben ser debidamente documentados.

Esta actividad está constituida por la revisión de entradas, como el resultado de la auditoría del SGSI, una realimentación de las partes interesadas, cambios que puedan afectar el SGSI, vulnerabilidades y riesgos que no se le dieron la adecuada importancia en el tratamiento de riesgos que se realizó anteriormente, entre otros casos, y nos dará ciertas salidas, como puede ser una actualización sobre la administración de los riesgos y las estrategias a considerar para su tratamiento, modificación de procedimientos y controles, una actualización del SGSI, entre otros. Esto dará como resultado el documento de administración de la revisión del SGSI, que incluye:

- Resultados de la revisión.
- Realimentación hacia las partes interesadas.
- Vulnerabilidades y amenazas que no se adecuan a la valoración de riesgos previa.
- Acciones preventivas y correctivas, entre otros.

4.1.5. Mejoras al SGSI

La organización debe encargarse de mejorar continuamente la eficiencia del SGSI a través del empleo de la política de seguridad de información, sus objetivos, el resultado de las auditorías, el análisis y monitoreo de eventos, las acciones preventivas y correctivas y revisiones de administración. Debe llevar a cabo acciones correctivas para eliminar las causas que no estén en conformidad con los

Tesis publicada con autorización del autor
No olvide citar esta tesis

requerimientos del SGSI para evitar que vuelvan a ocurrir los incidentes, y preventivas para eliminar la causa de potenciales amenazas y prevenir que ocurran.

4.2. Factores críticos de éxito para implementar el SGSI

Para poder implementar de manera satisfactoria un SGSI, se consideran ciertos factores críticos de éxito. En caso no se cumpla algunos de los factores a mostrar a continuación, es posible que actúen como un cuello de botella al momento de implementar el sistema. [14]

4.2.1. Compromiso de la dirección

Para poder implementar de manera satisfactoria un SGSI, es necesario contar con el compromiso formal y el total respaldo de la alta gerencia, respecto a la implementación. Esto va a brindar al oficial de seguridad responsable de la administración del sistema el "empowerment" necesario para poder implementar los controles que vaya a definir. Para ello, es necesario fijar y administrar los objetivos y propósitos del SGSI, los cuales deben estar descritos en términos del negocio.
Periódicamente se debe informar a la alta gerencia de los avances del SGSI y de las decisiones que se tomen.

4.2.2. Consideraciones financieras

Para poder implementar el SGSI, es necesario que se asignen los recursos necesarios para el mismo. Es recomendable que se cuente con un fondo destinado a la implementación de los controles que vaya a definir el oficial de seguridad de la empresa. En caso no se cuente con un fondo destinado al SGSI, se corre el riesgo de no mantener una estrategia de seguridad adecuada.
La labor del oficial de seguridad va a ser, en este caso, calcular el retorno de inversión de los controles e implementar aquellos que brinden una seguridad adecuada y que vayan alineados con los objetivos de la empresa.

4.2.3. Organización de la seguridad de información

Es importante para poder implementar el SGSI contar con una estrategia muy clara y precisa. Se deben definir los roles y responsabilidades, por ejemplo en una política de la empresa cuyo alcance sea a todos los colaboradores de la empresa, de aquellos actores que participen en la implementación del sistema. Esto incluye no

Tesis publicada con autorización del autor
No olvide citar esta tesis

solo al oficial de seguridad, sino también a los propietarios de información, custodios, usuarios, personal de TI con diferentes funciones, entre otros.

Adicionalmente, es importante formalizar el comité de seguridad dentro de la organización, ya que va a ser un medio por el que se va a presentar el avance del sistema a la alta gerencia y tratar temas relacionados a la seguridad de la compañía. En este comité puede estar presente no solo la alta gerencia, sino también todas las partes que guardan relación con temas de seguridad en la empresa (Riesgos, Auditoría, entre otras unidades).

4.2.4. Actividades específicas de la seguridad

Las actividades relacionadas a seguridad deben obedecer a las leyes y regulaciones sobre las que se rige el negocio. Para el caso de una compañía de seguros, se basa en el cumplimiento de la circular G140, elaborada por la Superintendencia de Banca y Seguros.

Para poder cumplir con la circular y contar con un adecuado SGSI, es recomendable seguir estándares ya definidos y aceptados por profesionales en la materia, como por ejemplo, el uso de Cobit y de la ISO27002. También existen buenas prácticas que pueden ayudar a complementar la relación de controles implementados por la organización.

4.2.5. Gestión de riesgos

Como se ha podido apreciar en el desarrollo del documento, uno de los hitos importantes en el diseño del SGSI es el análisis y el tratamiento de riesgos, por lo que es uno de los factores más importantes de éxito. Es fundamental contar con una metodología bien definida de evaluación de riesgos, definiendo los criterios de identificación y evaluación de riesgos.

De esta gestión va a depender que se definan los controles necesarios y adecuados en el SGSI para el tratamiento de los riesgos. Como un punto adicional, se recomienda que el oficial de seguridad reciba una capacitación en riesgos para que este paso se realice de una manera adecuada.

4.2.6. Involucrar a los stakeholders

Es importante contar con la participación de todo el personal de la compañía, desde la alta gerencia incluyendo a todos los empleados, tanto para la implementación de los controles como para acatar lo definido en las políticas de Seguridad. Es

Tesis publicada con autorización del autor
No olvide citar esta tesis

importante que la alta gerencia brinde su apoyo a Seguridad de la Información para poder implementar los ajustes y controles necesarios.

4.3. Selección de la plataforma de control y los objetivos de control

La plataforma de control seleccionada para el diseño del SGSI será el marco de control COBIT 4.1. Debido a que el sistema que se va a desarrollar en esta tesis es un Sistema de Gestión de Seguridad de Información, este va a estar enfocado básicamente en aquellos procesos de TI cuyo enfoque esté relacionado con los tres "pilares" de la seguridad de la información, que son: la integridad, la confidencialidad y la disponibilidad. Para esto se tomará en cuenta aquellos procesos de TI en cuyo enfoque se muestren como primario o como secundario, por último, si es que así se considere adecuado, según el giro del negocio, los pilares de seguridad de la información. En otros casos, puede ser que los procesos de TI no tengan que ver con ninguno de los tres enfoques mencionados, pero se incluirán para poder cumplir con la parte de administración de riesgos.

Por esta razón, los procesos de TI que actuarán como la plataforma de control del SGSI, y que serán especificados en la declaración de aplicabilidad, son los siguientes:

- PO2. Definir la arquitectura de la información
- PO4. Definir los procesos, organización y relaciones de TI
- PO6. Comunicar las aspiraciones y la dirección de la gerencia.
- PO8. Administrar la calidad.
- PO9. Evaluar y administrar los riesgos de TI.
- AI2. Adquirir y mantener software aplicativo.
- AI3. Adquirir y mantener infraestructura tecnológica.
- AI4. Facilitar la operación y el uso.
- AI6. Administrar cambios.
- AI7. Instalar y acreditar soluciones y cambios.
- DS1. Definir y administrar los niveles de servicio.
- DS2. Administrar los servicios de terceros.
- DS4. Garantizar la continuidad del servicio.
- DS5. Garantizar la seguridad de los sistemas.
- DS7. Educar y Entrenar a los usuarios.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- DS9. Administrar la configuración.
- DS10. Administración de problemas.
- DS11. Administración de datos.
- DS12. Administración del ambiente físico.
- DS13. Administración de operaciones.
- ME2. Monitorear y evaluar el control interno.

4.4. Declaración de aplicabilidad

La declaración de aplicabilidad o SOA (Statement of Applicability) se referencia en la cláusula 4.2.1j del estándar ISO/IEC 27001 y describe los objetivos de control y controles relevantes y aplicables al alcance del SGSI de la empresa y en función de la política y conclusiones del proceso de evaluación y tratamiento del riesgo.

Dado que en la tesis se va a trabajar en base a Cobit, se va a realizar la declaración de aplicabilidad sobre sus objetivos de control para luego poder realizar un cruce con la ISO27002 y posteriormente definir los controles para mitigar los riesgos identificados en los capítulos anteriores. El desarrollo de la declaración de aplicabilidad se puede apreciar en los anexos, en la sección "Declaración de Aplicabilidad".

Para la declaración de aplicabilidad, se han identificado los siguientes razones por las cuales se estaría aceptando un control o no:

- RL: Requerimientos legales
- OC: Obligaciones contractuales
- RN/BP: Requerimientos del negocio / Buenas prácticas
- RAR; Resultado del análisis de riesgo

Se puede apreciar parte de la declaración de aplicabilidad en la siguiente matriz, para un mayor detalle se puede visitar la sección de anexos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Procesos de TI	Objetivo de Control	Razón				Aplicabilidad
		RL	OC	RN/BP	RAR	
PO1 Definir un Plan Estratégico de TI	PO1.1 Administración del valor de TI					No aplica. Este objetivo de control se basa en definir un plan estratégico de TI, el cual no se encuentra en el alcance de un SGSI ya que el plan de seguridad está orientado al plan estratégico de TI y de la compañía.
	PO1.2 Alineación de TI con el Negocio					No aplica. Este objetivo de control se basa en definir un plan estratégico de TI, el cual no se encuentra en el alcance de un SGSI ya que el plan de seguridad está orientado al plan estratégico de TI y de la compañía.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

	PO1.3 Evaluación de desempeño y la capacidad actual					No aplica. Este objetivo de control se basa en definir un plan estratégico de TI, el cual no se encuentra en el alcance de un SGSI ya que el plan de seguridad está orientado al plan estratégico de TI y de la compañía.
	PO1.4 Plan estratégico de TI					No aplica. Este objetivo de control se basa en definir un plan estratégico de TI, el cual no se encuentra en el alcance de un SGSI ya que el plan de seguridad está orientado al plan estratégico de TI y de la compañía.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

	PO1.5 Planes tácticos de TI					No aplica. Este objetivo de control se basa en definir un plan estratégico de TI, el cual no se encuentra en el alcance de un SGSI ya que el plan de seguridad está orientado al plan estratégico de TI y de la compañía.
	PO1.6 Administración del portafolio de TI					No aplica. Este objetivo de control se basa en definir un plan estratégico de TI, el cual no se encuentra en el alcance de un SGSI ya que el plan de seguridad está orientado al plan estratégico de TI y de la compañía.

Tesis publicada con autorización del autor
No olvide citar esta tesis

PO2. Definir la arquitectura de la información	PO2.1 Modelo de arquitectura de información empresarial					No aplica. Este objetivo de control se basa en mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones que den soporte a la toma de decisiones, orientado al plan de TI, Si bien se debe verificar que la información se mantenga de forma íntegra al momento de realizar el diseño, esta verificación se considera en otros objetivos de control más específicos.
	PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	X		X	X	El objetivo de control aplica para el SGSI.
	PO2.3 Esquema de clasificación de datos	X		X	X	El objetivo de control aplica para el SGSI.
	PO2.4 Administración de Integridad	X		X	X	El objetivo de control aplica para el SGSI.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PO3. Determinar la dirección tecnológica	PO3.1 Planeación de la dirección tecnológica	X		X	X	El objetivo de control aplica para el SGSI.
	PO3.2 Plan de infraestructura tecnológica					No aplica. Este objetivo de control se basa en definir un plan de infraestructura tecnológica, el cual no se encuentra en el alcance de un SGSI ya que el plan de seguridad está orientado al plan estratégico de TI y de la compañía.
	PO3.3 Monitoreo de tendencias y regulaciones futuras			X		El objetivo de control aplica para el SGSI.
	PO3.4 Estándares tecnológicos		X	X	X	El objetivo de control aplica para el SGSI.
	PO3.5 Consejo de Arquitectura de TI			X		El objetivo de control aplica para el SGSI.
PO4. Definir los procesos, organización y relaciones de TI	PO4.1 Marco de trabajo de procesos de TI					No aplica. Este objetivo de control se basa en definir un marco de trabajo para ejecutar el plan estratégico de TI.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

	PO4.2 Comité estratégico de TI					No aplica para el desarrollo del SGSI. Este objetivo de control se basa en establecer un comité estratégico de TI a nivel de consejo para asegurar que el gobierno de TI se maneje de manera adecuada. No se encuentra orientado a temas de seguridad de la información.
	PO4.3 Comité directivo de TI			X		El objetivo de control aplica para el SGSI.
	PO4.4 Ubicación organizacional de la función de TI			X		El objetivo de control aplica para el SGSI.
	PO4.5 Estructura organizacional			X		El objetivo de control aplica para el SGSI.
	PO4.6 Establecimiento de roles y responsabilidades	X	X	X	X	El objetivo de control aplica para el SGSI.

Tesis publicada con autorización del autor
No olvide citar esta tesis

	PO4.7 Responsabilidad de aseguramiento de calidad de TI					No aplica. Este objetivo de control busca asegurar la calidad de TI, lo cual no es el enfoque de la solución que se plantea.
	PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento	X	X	X	X	El objetivo de control aplica para el SGSI.
	PO4.9 Propiedad de datos y de sistemas			X	X	El objetivo de control aplica para el SGSI.
	PO4.10 Supervisión			X	X	El objetivo de control aplica para el SGSI.

4.5. Diseño de controles para el SGSI

Luego de definir en la declaración de aplicabilidad que objetivos de control se van a incluir en el sistema, se procede a elaborar los distintos controles para cada uno de los objetivos seleccionados.

4.5.1. Mapeo entre Circular G140 e ISO27002

Para poder cumplir con el objetivo de la tesis, que es cumplir con lo estipulado en la circular G140, se va a realizar un cruce entre los dominios de la ISO y de la circular, a fin de ver las similitudes que tienen ambas. Si uno entra a ver el detalle de los controles, se puede apreciar que la circular tiene su base en la ISO27002.

El cruce realizado entre los dominios de ambos documentos es el siguiente:

Tesis publicada con autorización del autor
No olvide citar esta tesis

Circular G 140.2009	*ISO 27002:2005*
3. Sistema de gestión de la seguridad de la información	01. Políticas de Seguridad
4. Estructura organizacional	02. Organización de Seguridad de Información
5.4. Controles de Seguridad de información / Inventario de activos y clasificación de la información	03. Administración de Activos
5.2. Controles de Seguridad de información / Seguridad de personal	04. Seguridad de Recursos Humanos
5.3. Controles de Seguridad de información / Seguridad física y ambiental	05. Seguridad física y ambiental
5.5. Controles de Seguridad de información / Administración de las operaciones y comunicaciones	06. Gestión de Comunicaciones y Operaciones
5.7. Controles de Seguridad de información / Procedimientos de respaldo	06. Gestión de Comunicaciones y Operaciones
5.1. Controles de Seguridad de información / Seguridad lógica	07. Control de Accesos
5.6. Controles de Seguridad de información / Adquisición, desarrollo y mantenimiento de sistemas informáticos	08. Adquisición, Desarrollo y Mantenimiento de Sistemas de información
5.8. Controles de Seguridad de información / Gestión de incidentes de seguridad de información	09. Gestión de Incidentes de Seguridad de Información 10. Administración de Continuidad del Negocio
5.9. Controles de Seguridad de información / Cumplimiento normativo	11. Cumplimiento
5.10. Controles de Seguridad de información / Privacidad de la información	06. Gestión de Comunicaciones y Operaciones
6. Seguridad de operaciones de transferencia de fondos por canales electrónicos	06. Gestión de Comunicaciones y Operaciones

Tabla 3. Mapeo entre la Circular G140 e ISO27002

4.5.2. Mapeo entre Cobit e ISO27002

El mapeo entre Cobit y la ISO27002 es el trabajo principal en el desarrollo del SGSI. Al realizar el mapeo, desarrollado en la sección de anexos, se va a englobar todo aquello que ya se ha trabajado en los capítulos anteriores y se definirán distintos controles para mitigar los riesgos ya identificados.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Página dejada en blanco intencionalmente

Tesis publicada con autorización del autor
No olvide citar esta tesis

Objetivo de control Cobit 4.1	Controles ISO27002:2005	Fuente de origen del riesgo	Causa	Riesgo asociado	Control a tomar	Tipo de Control	Rol responsable sugerido	Estrategia sugerida para el riesgo
PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	7.1.1 Inventario de los activos	Proceso	No contar con una clasificación de activos que permita identificar la criticidad de los mismos al momento de recuperarse de un incidente.	Disponibilidad de la información	Mantener un inventario de activos, incluyendo activos de información, físicos, aplicaciones, entre otros.	Preventivo	Cumplimiento, Auditoría, Riesgo y Seguridad, Dueño de Proceso de Negocio	Mitigar
		Proceso	No contar con una clasificación de activos que permita gestionar un adecuado control de acceso a los mismos.	Integridad de la información se ve afectada Confidencialidad de la información se ve afectada.	Clasificar los activos con los PDI para tomar las acciones necesarias para su protección, dependiendo de su criticidad.	Preventivo - Correctivo	Cumplimiento, Auditoría, Riesgo y Seguridad, Dueño de Proceso de Negocio	Mitigar
	11.1.1 Política de control de accesos	Proceso	Inadeacuado proceso de control de accesos.	Integridad de la información se ve afectada Confidencialidad de la información se ve afectada.	Definir una política de control de accesos indicando los lineamientos para los distintos grupos de usuarios.	Preventivo	Cumplimiento, Auditoría, Riesgo y Seguridad.	Mitigar
PO2.3 Esquema de clasificación de datos	7.2.1 Lineamientos de clasificación	Sistemas de información	Inadecuado control de acceso.	Modificación no autorizada de información.	Realizar una clasificación de activos de información a nivel de sistemas y aplicaciones de la empresa para poder soportar procesos como el de administración de accesos. La clasificación debe de ser realizada con ayuda del propietario de información, para que pueda indicar si la información es pública, privada o confidencial.	Preventivo - Correctivo	Cumplimiento, Auditoría, Riesgo y Seguridad, Dueño de Proceso de Negocio	Mitigar
	10.7.1 Gestión de medios removibles	Proceso	Procedimiento deficiente para dar de baja a los equipos.	Información de la compañía puede caer en manos de la competencia	Desarrollar una política para eliminación segura de data para que esta no pueda ser reconstruida. Controlar que las personas encargadas de esta tarea cumplen los lineamientos formulados en la política.	Preventivo	Cumplimiento, Auditoría, Riesgo y Seguridad.	Eliminar

Tesis publicada con autorización del autor
No olvide citar esta tesis

	10.8.1 Políticas y procedimientos de intercambio de información	Fuente externa	Información de la empresa que pudo ser modificada por terceros de manera indebida	Pérdida de integridad de la información.	El uso de certificados digitales para proteger el canal de envío de información.	Preventivo	Jefe de Operaciones, Seguridad	Eliminar
		Sistemas de Información	Ataque informático en contra de la información de la empresa.	Pérdida parcial o total de la información a causa de ataques de terceros				
		Fuente externa	Información de la empresa que pudo ser modificada por terceros de manera indebida	Pérdida de integridad de la información.	Desarrollar una política en el que se tomen todas las consideraciones para el adecuado intercambio de información, controlando que esta pueda ser modificada, copiada, interceptada, destruida, entre otros. También debe de considerar el uso aceptable de los medios de comunicación, considerar los riesgos que trae el uso de una conexión inalámbrica y definir responsabilidades con los usuarios, ya sean terceros o personal de la compañía.	Preventivo	Cumplimiento, Auditoría, Riesgo y Seguridad.	Mitigar
		Sistemas de Información	Ataque informático en contra de la información de la empresa.	Pérdida parcial o total de la información a causa de ataques de terceros				
	10.8.2 Acuerdos de intercambio	Fuente externa	Información accedida de manera indebida por terceros	Pérdida de confidencialidad de información.	Incluir acuerdos de intercambio de información en los contratos que se realicen con terceros, incluyendo cláusulas donde se mencionen represalias en caso no se cumplan los mismos.	Preventivo	Legal	Mitigar
	11.1.1 Política de control de accesos	Proceso	Inadeacuado proceso de control de accesos.	· Integridad de la información se ve afectada, · Confidencialidad de la información se ve afectada,	· Definir una política de control de accesos indicando los lineamientos para los distintos grupos de usuarios.	Preventivo	Cumplimiento, Auditoría, Riesgo y Seguridad.	Mitigar
PO2.4 Administración de Integridad	11.1.1 Política de control de	Proceso	Inadeacuado proceso de control de accesos.	· Integridad de la información se ve afectada,	· Definir una política de control de accesos indicando los lineamientos	Preventivo	Cumplimiento, Auditoría, Riesgo y Seguridad.	Mitigar

Tesis publicada con autorización del autor
No olvide citar esta tesis

	accesos			. Confidencialidad de la información se ve afectada,	para los distintos grupos de usuarios.			
PO3.1 Planeación de la dirección tecnológica	5.1.2 Revisión de la política de seguridad de información	Proceso	Políticas de SI desactualizadas	Incumplimiento de regulaciones.	Revisar periódicamente las políticas base del SGSI y siempre que se considere necesario.	Preventivo - Detectivo - Correctivo	Cumplimiento, Auditoría, Riesgo y Seguridad.	Eliminar
	14.1.1 Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio	Sistemas de información	Ausencia de un centro alterno de cómputo para restablecer el servicio en caso de un incidente.	Perdida de disponibilidad de información	Contar con un centro de operaciones de contingencia.	Preventivo	Jefe de Operaciones	Mitigar
		Sistemas de información	No hay un respaldo de la información de la empresa.	Perdida de disponibilidad de información				
		Fuentes externas	Ataque de denegación de servicios por parte de externos.	Interrupción del servicio				
		Sistemas de información	No hay un respaldo de la información de la empresa.	Perdida de disponibilidad de información	Probar periódicamente el BCP y el DRP para estar seguros que se encuentran bien planificados en caso de un incidente.	Preventivo - Detectivo - Correctivo	Riesgos, Jefe de Operaciones	Mitigar
		Fuente externa	Desastre natural	Pérdida parcial o total de la información a causa de un desastre natural				
		Fuentes externas	Ataque de denegación de servicios por parte de externos.	Interrupción del servicio				
		Sistemas de información	No hay un respaldo de la información de la empresa.	Perdida de disponibilidad de información	Considerar un presupuesto a nivel de toda la organización para garantizar el plan de continuidad de negocio. Es necesario que se incluya dentro del plan de contiuidad de negocio un plan de recuperación de desastres manejado para recuperar las aplicaciones principales.	Preventivo	CEO	Mitigar
		Fuente externa	Desastre natural	Pérdida parcial o total de la información a causa de un desastre natural				
		Fuentes externas	Ataque de denegación de servicios por parte de externos.	Interrupción del servicio				

Tesis publicada con autorización del autor
No olvide citar esta tesis

	14.1.5 Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio	Sistemas de información	Ausencia de un centro alterno de cómputo para restablecer el servicio en caso de un incidente.	Perdida de disponibilidad de información	Contar con un centro de operaciones de contingencia.	Preventivo	Jefe de Operaciones	Mitigar
		Sistemas de información	No hay un respaldo de la información de la empresa.	Perdida de disponibilidad de información				
		Fuentes externas	Ataque de denegación de servicios por parte de externos.	Interrupción del servicio				
		Sistemas de información	No hay un respaldo de la información de la empresa.	Perdida de disponibilidad de información	Probar periódicamente el BCP y el DRP para estar seguros que se encuentran bien planificados en caso de un incidente.	Preventivo - Detectivo - Correctivo	Riesgos, Jefe de Operaciones	Mitigar
		Fuente externa	Desastre natural	Pérdida parcial o total de la información a causa de un desastre natural				
		Fuentes externas	Ataque de denegación de servicios por parte de externos.	Interrupción del servicio				
		Sistemas de información	No hay un respaldo de la información de la empresa.	Perdida de disponibilidad de información	Considerar un presupuesto a nivel de toda la organización para garantizar el plan de continuidad de negocio. Es necesario que se incluya dentro del plan de contiuidad de negocio un plan de recuperación de desastres manejado para recuperar las aplicaciones principales.	Preventivo	CEO	Mitigar
		Fuente externa	Desastre natural	Pérdida parcial o total de la información a causa de un desastre natural				
		Fuentes externas	Ataque de denegación de servicios por parte de externos.	Interrupción del servicio				

Tesis publicada con autorización del autor
No olvide citar esta tesis

PO3.3 Monitoreo de tendencias y regulaciones futuras	6.1.1 Compromiso de la gerencia con la seguridad de la información	Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones	Involucrar y comprometer a la alta gerencia con el plan de seguridad de información. Para ello, se debe de formalizar un Comité de Seguridad que se debe de realizar periódicamente (2 o 3 veces al año) donde se presentarán los avances del ISMS.	Preventivo	Seguridad	Eliminar
PO3.4 Estándares tecnológicos	10.3.2 Aceptación del sistema	Proceso	Modificación sobre las aplicaciones importantes en el negocio sin evaluar el impacto del cambio.	Problemas en las aplicaciones "core" del negocio.	La generación de un comité de pases a producción para regular los pases sobre las aplicaciones y nuevos cambios que se vayan a realizar.	Preventivo	Jefe de Desarrollo, PMO	Mitigar
					Contar con ambientes de desarrollo, pre producción y producción para el desarrollo de aplicaciones y posibles cambios sobre las mismas.	Preventivo - Correctivo	Jefe de Desarrollo	Mitigar
	10.8.2 Acuerdos de intercambio	Fuente externa	Información accedida de manera indebida por terceros	Pérdida de confidencialidad de información.	Incluir acuerdos de intercambio de información en los contratos que se realicen con terceros, incluyendo cláusulas donde se mencionen represalias en caso no se cumplan los mismos.	Preventivo	Legal	Mitigar
	11.7.2 Tele-trabajo	Red	Red insegura, facilita el ataque de terceros para que puedan modificar información.	Modificación no autorizada de información.	Acceso remoto usando autenticación doble (clave estática y dinámica)	Preventivo	Jefe de Desarrollo, Jefe de Arquitectura, Seguridad	Mitigar
PO3.5 Consejo de Arquitectura de TI	6.1.1 Compromiso de la gerencia con la seguridad de la información	Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones	Involucrar y comprometer a la alta gerencia con el plan de seguridad de información. Para ello, se debe de formalizar un Comité de Seguridad que se debe de realizar periódicamente (2 o 3 veces al año) donde se presentarán los avances del ISMS.	Preventivo	Seguridad	Eliminar

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PO4.3 Comité directivo de TI	6.1.1 Compromiso de la gerencia con la seguridad de la información	Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones	Involucrar y comprometer a la alta gerencia con el plan de seguridad de información. Para ello, se debe de formalizar un Comité de Seguridad que se debe de realizar periódicamente (2 o 3 veces al año) donde se presentarán los avances del ISMS.	Preventivo	Seguridad	Eliminar
	6.1.4 Autorización de proceso para facilidades procesadoras de información	Sistemas de información	Mala atención por parte de la plataforma, debido a errores en el sistema.	Mala atención por parte de la plataforma, debido a errores en el sistema.	Formalizar que cada instalación de HW o SW debe de contar con una evaluación previa para asegurar compatibilidad con la plataforma en uso. Se puede utilizar una plantilla de evaluación estándar que sirva incluso para poder comparar varios proveedores distintos y el nivel de seguridad que son capaces de proveer.	Preventivo	Jefe de Arquitectura, Seguridad	Mitigar
				Servicio inoportuno y demorado a los clientes.				
			Fallas en el sistema.	Pérdida o daño de capacidades operativas a causa de problemas con los sistemas de información				
		Sistemas de información	Inadecuado control de acceso.	Modificación no autorizada de información.	Formalizar que cada pedido cuente con la aprobación de la gerencia del usuario solicitante.	Preventivo	Seguridad	Mitigar
PO4.4 Ubicación organizacional de la función de TI	6.1.1 Compromiso de la gerencia con la seguridad de la información	Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones	Involucrar y comprometer a la alta gerencia con el plan de seguridad de información. Para ello, se debe de formalizar un Comité de Seguridad que se debe de realizar periódicamente (2 o 3 veces al año) donde se presentarán los avances del ISMS.	Preventivo	Seguridad	Eliminar

Tesis publicada con autorización del autor
No olvide citar esta tesis

	6.1.2 Coordinación de la seguridad de información	Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones	Involucrar y comprometer a la alta gerencia con el plan de seguridad de información. Para ello, se debe de formalizar un Comité de Seguridad que se debe de realizar periódicamente (2 o 3 veces al año) donde se presentarán los avances del ISMS.	Preventivo	Seguridad	Eliminar
		Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones	Promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización.	Preventivo	Seguridad, RRHH	Mitigar
	6.1.3 Asignación de las responsabilidades de la seguridad de la información	Sistemas de información	No hay un respaldo de la información de la empresa.	Perdida de disponibilidad de información	Definir responsables y responsabilidades para el desarrollo del plan de continuidad de negocios (BCP).	Preventivo	Riesgos	Mitigar
		Fuente externa	Desastre natural	Pérdida parcial o total de la información a causa de un desastre natural				
		Fuentes externas	Ataque de denegación de servicios por parte de externos.	Interrupción del servicio				
		Sistemas de información	Inadecuado control de acceso.	Modificación no autorizada de información.	Definir e incluir en las normas y politicas de seguridad las funciones y responsabilidades para los propietarios de informacion asi como de los usuarios que utilizan los diferentes activos de información.	Preventivo	Cumplimiento, Auditoría, Riesgo y Seguridad, Dueño de Proceso de Negocio	Mitigar
	6.1.4 Autorización de proceso para facilidades procesadoras de información	Sistemas de información	Mala atención por parte de la plataforma, debido a errores en el sistema.	Mala atención por parte de la plataforma, debido a errores en el sistema.	Formalizar que cada instalación de HW o SW debe de contar con una evaluación previa para asegurar compatibilidad con la plataforma en uso. Se puede utilizar una plantilla de evaluación estándar que sirva incluso para poder comparar varios	Preventivo	Jefe de Arquitectura, Seguridad	Mitigar

Tesis publicada con autorización del autor
No olvide citar esta tesis

				Servicio inoportuno y demorado a los clientes.	proveedores distintos y el nivel de seguridad que son capaces de proveer.			
			Fallas en el sistema.	Pérdida o daño de capacidades operativas a causa de problemas con los sistemas de información				
		Sistemas de información	Inadecuado control de acceso.	Modificación no autorizada de información.	Formalizar que cada pedido cuente con la aprobación de la gerencia del usuario solicitante.	Preventivo	Seguridad	Mitigar
PO4.5 Estructura organizacional	6.1.1 Compromiso de la gerencia con la seguridad de la información	Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones	Involucrar y comprometer a la alta gerencia con el plan de seguridad de información. Para ello, se debe de formalizar un Comité de Seguridad que se debe de realizar periódicamente (2 o 3 veces al año) donde se presentarán los avances del ISMS.	Preventivo	Seguridad	Eliminar
	6.1.2 Coordinación de la seguridad de información	Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones	Involucrar y comprometer a la alta gerencia con el plan de seguridad de información. Para ello, se debe de formalizar un Comité de Seguridad que se debe de realizar periódicamente (2 o 3 veces al año) donde se presentarán los avances del ISMS.	Preventivo	Seguridad	Eliminar
		Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones	Promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización.	Preventivo	Seguridad, RRHH	Mitigar

Tesis publicada con autorización del autor
No olvide citar esta tesis

PO4.6 Establecimiento de roles y responsabilidades	6.1.2 Coordinación de la seguridad de información	Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones	Involucrar y comprometer a la alta gerencia con el plan de seguridad de información. Para ello, se debe de formalizar un Comité de Seguridad que se debe de realizar periódicamente (2 o 3 veces al año) donde se presentarán los avances del ISMS.	Preventivo	Seguridad	Eliminar
		Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones	Promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización.	Preventivo	Seguridad, RRHH	Mitigar
	6.1.3 Asignación de las responsabilidades de la seguridad de la información	Sistemas de información	No hay un respaldo de la información de la empresa.	Perdida de disponibilidad de información	Definir responsables y responsabilidades para el desarrollo del plan de continuidad de negocios (BCP).	Preventivo	Riesgos	Mitigar
		Fuente externa	Desastre natural	Pérdida parcial o total de la información a causa de un desastre natural				
		Fuentes externas	Ataque de denegación de servicios por parte de externos.	Interrupción del servicio				
		Sistemas de información	Inadecuado control de acceso.	Modificación no autorizada de información.	Definir e incluir en las normas y politicas de seguridad las funciones y responsabilidades para los propietarios de informacion asi como de los usuarios que utilizan los diferentes activos de información.	Preventivo	Seguridad	Mitigar
	6.1.5 Acuerdos de confidencialidad	Fuente externa	Incumplimiento de contrato por parte de terceros	Mal uso de la información de la compañía.	Incluir acuerdos de confidencialidad de manera obligatoria en los contratos de la compañía en los que se vaya a manejar información sensible (incluye personal de la compañía y terceros). Debe estar incluido en las políticas de la compañía como lineamiento a seguir.	Preventivo	Legal	Mitigar

Tesis publicada con autorización del autor
No olvide citar esta tesis

	8.1.1 Roles y responsabilidades	Proceso	Desconocimiento de regulaciones que aplican al giro de negocio.	Incumplimiento de regulaciones	Definir una política de responsabilidad y funciones de seguridad de información donde se definan las responsailidades y funciones del equipo de seguridad de información, propietarios de información, administradores de accesos, colaboradores y terceros.	Preventivo	Cumplimiento, Auditoría, Riesgo y Seguridad.	Eliminar
	8.1.2 Investigación de antecedentes	Personas	Falta de entrenamiento de personal	No reclutar, desarrollar o retener a los empleados que cuenten con habilidades o conocimientos apropiados.	Validar la información del currículum vitae del personal a contratar.	Preventivo	RRHH	Mitigar

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

5. Desarrollo de política base para el SGSI

EL SGSI se basa en un conjunto de políticas, estándares, y procedimientos que de alguna manera regulan que los controles implementados se lleven a cabo por las distintas áreas y que todo trabajador de la compañía debe seguir. A continuación se desarrollará la política de Seguridad de Información, que es considerada la base del SGSI a desarrollar:

5.1. Política de Seguridad de Información

Alcance

Toda la compañía

Lineamientos Generales

a) La alta gerencia se compromete a cumplir las políticas de seguridad de información de la empresa. Del mismo modo, es obligatorio que todo el

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

personal también las cumpla y colabore con la implementación de los controles cada vez que seguridad lo solicite.

b) Seguridad de Información tiene como objetivo:

- La protección de la información contra accesos no autorizados.
- La protección contra la modificación de información durante su procesamiento, almacenamiento o transmisión.
- La protección contra la negación de servicio a usuarios autorizados o prestación de servicio a usuarios no autorizados, incluyendo las medidas necesarias para la detección, documentación y registro de tales amenazas.
- La protección de la privacidad de la información personal de los clientes.

c) Seguridad de Información difundirá las funciones y responsabilidades que todo el personal de la compañía debe conocer y seguir para el buen uso de la información.

d) Toda información es propiedad de la compañía, independientemente del medio que la contenga, por lo que debe ser protegida de modificación, eliminación y conocimiento por personas ajenas a la compañía o a las funciones asignadas.

5.2. Políticas adicionales

Políticas Generales de Administración de Accesos

a) Los administradores de accesos, tienen como principal responsabilidad contar con un proceso uniforme para la administración a los distintos recursos informáticos de la empresa.

b) Todo medio de información, aplicativo o recurso de computador, catalogado como crítico, debe tener un líder usuario o usuario propietario quien será el responsable de la implementación de las políticas de seguridad relacionadas a ese aplicativo en particular.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

c) Los líderes usuarios (jefes de las áreas) o usuarios propietarios tienen la responsabilidad de determinar cómo serán administrados los recursos de sistemas bajo su responsabilidad, en coordinación con Seguridad de Información.

d) La administración de seguridad debe ser auditada y revisada para asegurar que los procesos a su cargo se realicen de manera eficiente y efectiva.

Políticas Generales de Identificación de Usuarios

a) Para el acceso a todo sistema de información cada empleado debe tener una identificación y contraseñas únicas que deberán ser validados con mecanismos de autenticidad. Los líderes usuarios o propietarios de Información tienen la responsabilidad de definir los requerimientos de identificación y autenticación de los usuarios.

b) Para aquellos sistemas donde el acceso se ofrece directamente a clientes o personas que no son empleados de la compañía se debe considerar la existencia de un código de identificación único por usuario y se les deberá proveer de guías sobre su uso y responsabilidades.

Políticas Generales de Acceso a Recursos

a) Todo acceso a la información deberá ser a través de una aplicación y estará protegida por medio de mecanismos de control de acceso y controles de acceso físico a los recursos de cómputo.

b) Para los accesos que se den por excepción, la solicitud debe de contar con la autorización del propietario de información correspondiente.

c) Personal del área de Tecnología no deberá realizar modificaciones a los ambientes de producción sin previo anuncio de un pase y cumpliendo con las autorizaciones respectivas.

Políticas Generales de Clasificación de Activos

a) Definir un método de clasificación de los Activos de Información de la empresa, para su protección frente a pérdida, divulgación no autorizada o

Tesis publicada con autorización del autor
No olvide citar esta tesis

cualquier otra forma de uso indebido, ya sea de modo accidental o intencionado.

b) Todo medio de información, aplicativo o recurso de computador, catalogado como crítico, debe tener un Propietario de Información, quienes determinarán la confidencialidad requerida para los recursos bajo su propiedad, en función a la importancia de la información y de los riesgos a los cuales está expuesto.

c) Antes de que alguna información se clasifique, se debe realizar un inventario de Activos de Información asociados a cada Sistema de Información.

d) Las consideraciones de seguridad que se deben tener presente para clasificar la información son las siguientes:

- Disponibilidad: Repercusión en el negocio, si la información no está disponible para su uso.
- Confidencialidad: Repercusión en el negocio, si la información llega a manos no autorizadas.
- Integridad: Repercusión en el negocio, si la información errónea es usada para la toma de decisiones.
- Privacidad: Repercusión en el negocio, si la información personal específica de cliente es expuesta.

e) De acuerdo a estas consideraciones, la información se clasifica en: pública, privada y confidencial.

- Pública: Información de carácter general, es decir, de conocimiento del personal de la empresa y de los clientes.
- Privada: Información cuya difusión deberá ser solo de carácter interno de la compañía, quedando prohibida su difusión, divulgación o modificación fuera de la misma. Su destrucción, alteración o difusión indebida puede comprometer, con alta probabilidad, operaciones esenciales.
- Confidencial: Información cuya existencia y contenido deberá recaer en un selecto número de personas o áreas específicas de la compañía, las que a su vez están prohibidas de divulgar, reproducir, modificar o destruir si no

Tesis publicada con autorización del autor
No olvide citar esta tesis

están autorizadas. Su destrucción, alteración o difusión indebida puede ocasionar, con alta probabilidad, pérdidas económicas importantes

Políticas Generales de Alertas, Auditorias y Cumplimiento

a) La administración de seguridad de las aplicaciones así como de los sistemas debe ser auditada y revisada para asegurar que los procesos involucrados se realicen de manera correcta.

b) Las aplicaciones deben incluir dentro de sus especificaciones funcionales y técnicas la definición de logs, pistas de auditoría y alertas para eventos críticos que permitan realizar un análisis forense (investigación por algún incidente).

c) La responsabilidad del cumplimiento de las normas es de todos los empleados.

Políticas Generales de Capacitación

a) Se incorporará el Programa de Capacitación de Seguridad de Información, que comprenderá un conjunto de acciones que permitirán:

- Generar en los empleados, desde el más alto nivel de dirección hasta los empleados temporales, una conciencia de seguridad y lograr su efectiva colaboración en el uso adecuado de los Sistemas y la protección de los activos de información de la compañía.
- Mantener actualizados a los empleados con relación a las políticas, normas, procedimientos y estándares de Seguridad de Información de la organización y las razones para ser utilizadas.

c) Se deberá desarrollar permanentemente acciones de capacitación al personal de la compañía en temas relacionados a la Seguridad de Información, cuyos objetivos son:

- Identificar las responsabilidades de cada empleado para el aseguramiento de los activos de información.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Proporcionar conocimientos en Seguridad de Información a los empleados para la buena toma de decisiones.

Políticas Generales de Privacidad

a) Todos los usuarios de información, proveedores y otros individuos con acceso a información de identificación individual deben mantener la privacidad de esta información constantemente.

b) Es responsabilidad de la compañía hacia sus clientes, empleados, proveedores y socios de negocios el mantener la privacidad de la información personal confidencial utilizada para el desarrollo del negocio.

c) El mantenimiento de la privacidad de la información confidencial requiere de los siguientes controles y medidas de seguridad como:

- Usar la información solamente para el propósito para el cual se recopiló.
- Mantener la información solamente por el tiempo requerido por las regulaciones vigentes o por el tiempo que sea relevante para el propósito inicial.
- No debe ser expuesta sin contar con la debida autorización y/o consentimiento de la persona, salvo casos en que la regulación lo exija o permita.
- Debe encontrarse disponible para que el individuo a quién pertenecen los datos pueda revisarla y copiarla.
- Debe ser corregida en caso se encuentren errores o si estos son identificados por el individuo a quien le pertenecen los datos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

6. Conclusiones

De acuerdo con lo expuesto en la presente tesis, actualmente se vive en una época en la que la información y los datos poseen una importancia decisiva en la gran mayoría de compañías, convirtiéndose así en su activo más importante. Por ejemplo, si en algún momento se da un terremoto y se cae el edificio de la compañía, se puede volver a reconstruir; si se realiza una mala inversión en la bolsa, se puede volver a recuperar el dinero. En cambio, si llegamos a perder la información de la compañía, es muy probable que no podamos volver a recuperarla si no se tienen las consideraciones debidas, con lo que es probable que la empresa deje de operar.

Partiendo de esta premisa, es importante contar con un Sistema de Gestión de Seguridad de la Información para poder asegurar, a un nivel aceptable, la información de la compañía y, dado que se trata de una compañía de seguros peruana, poder cumplir con las regulaciones de la SBS cumpliendo con el contenido de la circular G-140 y evitar así que la compañía incumpla con las regulaciones de la superintendencia.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Para poder desarrollar el sistema, es necesario poder conocer los procesos de la compañía. En este documento se consideraron los procesos que tiene una compañía de seguros en general, pero es importante considerar siempre que el SGSI debe estar enfocado en las necesidades del negocio. Es decir, si la compañía considera un proceso en particular como crítico, se deben implementar controles necesarios para asegurar el mismo.

El desarrollo del BIA es importante para el posterior análisis de riesgos. En él se identifican los riesgos asociados a los distintos procesos y la criticidad de los mismos, así como los recursos afectados en caso de un incidente de seguridad. El BIA también se utiliza como insumo para el desarrollo del plan de continuidad de negocios, que no ha sido parte del alcance de la tesis, y que va a ayudar a identificar aquellos recursos que se deben de recuperar para que el proceso se encuentre operativo una vez más. Una vez que desarrollamos el BIA, es necesario realizar un análisis de los riesgos identificados. Para ello, se puede establecer un comité, formado por personas que cuenten con la experiencia y el conocimiento necesario del negocio, que ayude a identificar los riesgos que afectan a la compañía. La participación de diferentes personas dentro de la compañía en el comité va a permitir identificar mejor los riesgos. Para esto, es importante que sean personas que tengan un conocimiento amplio sobre los distintos procesos de la compañía o sean especialistas sobre procesos específicos.

Una vez identificados los riesgos, se procede a desarrollar los controles para el SGSI. Antes que nada, es indispensable obtener el apoyo de la alta gerencia haciéndoles entender la importancia que tiene la seguridad de la información en toda compañía. Con el apoyo de la alta gerencia, podemos asegurar que el personal de la compañía va a seguir las políticas y procedimientos de seguridad de información que se vayan a publicar como parte del SGSI, así como los controles, lineamientos, estándares, entre otros que se puedan definir.

Para poder brindar un nivel aceptable de seguridad a la compañía, todo SGSI se debe basar en estándares y buenas prácticas orientadas a seguridad de la información que nos indican las consideraciones que debemos de tener en diferentes aspectos. En el caso del desarrollo de la tesis, se utilizó tanto Cobit 4.1 como el estándar ISO/IEC 27001:2005 y el ISO/IEC 27002:2005 para armar nuestro marco de control y poder definir los controles a seguir para el aseguramiento de la información de la compañía y el cumplimiento de la regulación impuesta por la SBS.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Se puede asegurar que la solución planteada (con la solución se hace referencia al SGSI) en la tesis es válida ya que, a nivel mundial, miles de empresas adoptan estas metodologías, estándares y demás con muy buenos resultados. Hay que recalcar que todas ellas, o han sido desarrolladas por expertos a nivel mundial en el rubro de la seguridad informática y temas afines, o bien se han desarrollado en base a buenas prácticas reconocidas y probadas a nivel mundial por diversas empresas con buenos resultados

Con un SGSI como el expuesto en la tesis se pueden solucionar los siguientes problemas:

- Cumplir con la normativa impuesta por la SBS (la circular G140) para todas las compañías de seguros que operen en territorio peruano.
- Brindar un nivel aceptable de seguridad con relación a la información que maneja la empresa, evitando incidentes que puedan afectar en la operativa diaria de la misma.
- Contar con un modelo que se amolde al paso del tiempo y se pueda actualizar siempre, debido a las revisiones periódicas a las que se ve sujeto el SGSI.

Por último, como comentario adicional, hay que recalcar que de nada sirve contar con un SGSI que consideren todos los posibles riesgos y controles para mitigarlos o contar con toda la tecnología posible para asegurar la información de la compañía si no se da una debida importancia a la seguridad de la información por parte de la alta gerencia y no se cumplen las políticas y procedimientos establecidos por parte del personal de la empresa.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

7. Recomendaciones

Se recomienda a todas aquellas compañías que se encuentran regidas bajo la Superintendencia de Banca y Seguros que implementen un SGSI, no solo para cumplir con la circular vigente, la G140, para evitar incumplimientos que puedan llevar a sanciones por parte de este organismo, sino también porque manejan información sensible que debe tener cierto cuidado para evitar que los clientes se vean afectados.

De igual forma, se recomienda a todas las demás empresas de los distintos rubros a contar con un SGSI, ya que es importante que la información que manejan y que mueve su negocio se encuentre debidamente protegida, para evitar pérdidas de ventaja competitiva y, en el peor de los casos, el paro de la empresa. La información, en la actualidad, es lo único que mueve a la mayoría de las empresas. Si pasa un desastre y se pierde el edificio de la compañía se puede recuperar (lo más probable es que esté asegurado). Si asaltan a una empresa se puede recuperar

Tesis publicada con autorización del autor
No olvide citar esta tesis

una parte o todo el dinero, según el seguro con el que se cuente, pero si se pierde la información de la compañía simplemente la empresa deja de operar.

Para poder implementar adecuadamente el SGSI, se recomienda utilizar estándares y buenas prácticas que sean ampliamente aceptadas. No necesariamente se tiene que aplicar lo que se ha mostrado en la tesis, ya que existe no una única forma de implementar un SGSI. Es importante usar los estándares y buenas prácticas de guía, pero no se debe implementar todo al pie de la letra. La implementación va a depender de las necesidades de la empresa. Cabe resaltar que estos estándares te indican que es aquello que se debe controlar, pero no indica el cómo. Acá entra a tallar la imaginación del oficial de seguridad a cargo en la compañía.

Para aquellas empresas que cuenten con un SGSI ya implementado, se les recomienda que el enfoque de su SGSI se encuentre alineado con las necesidades del negocio. Esto es importante ya que el desarrollo del plan de seguridad en la empresa no debe ser aislado de sus objetivos estratégicos. Adicionalmente, se debe tratar de obtener un retorno de inversión que justifique, de alguna manera, los gastos realizados en el año.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

8. Referencias Bibliográficas

[1] SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP
Proyecto de circular referida a la gestión de la seguridad de la información
http://www.sbs.gob.pe/PortalSBS/PreProyectos/normas/proyecto6/proyecto.pdf
2008

[2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ISO27000
www.iso27000.es
2008

[3] ADMINISTRACION DE RIESGOS
AS/NZS 4360
2004

[4] IT GOVERNANCE INSTITUTE
CobiT4.1.pdf
http://www.isaca.org

Código de campo cambiado

Tesis publicada con autorización del autor
No olvide citar esta tesis

[5] ITGI / OGC
ALIGNING COBIT® 4.1, ITIL® V3 AND ISO/IEC 27002 FOR BUSINESS BENEFIT
http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=46288
2008

[6] CORLETTI, ALEJANDRO
ISO 27001: LOS CONTROLES
http://www.kriptopolis.org/iso-27001-los-controles-parte-ii
2006

[7] NOXGLOBE
CONOZCA COBIT
http://www.noxglobe.com/modules/articles/cobit/

[8] PUCP
Capítulo 1. Seguridad Informática.
Curso : Seguridad Computacional
2009

[9] CONSEJO SUPERIOR DE ADMINISTRACION ELECTRONICA
METODOLOGIA DE ANALISIS Y GESTION DE RIESGOS DE LOS SISTEMAS DE INFORMACION
http://www.csi.map.es/csi/pdf/magerit_v2/metodo-v10b.PDF
http://www.csi.map.es/csi/pdf/magerit_v2/catalogo-v10.PDF
http://www.csi.map.es/csi/pdf/magerit_v2/tecnicas-v10.PDF
http://www.alertaantivirus.es/seguridad/ver_pag.html?tema=S&articulo=3&pagina=0

[10] SEMA GROUP
Metodología MAGERIT v1.0
http://ec.europa.eu/idabc/servlets/Doc?id=22813

[11] ITLP
CONTROL
http://sistemas.itlp.edu.mx/tutoriales/procesoadmvo/tema6_1.htm

Código de campo cambiado

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

[12] OSIATIS
http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_continuidad_del_servicio/proceso_gestion_de_la_continuidad_del_servicio/analisis_impacto_continuidad_del_servicio.php

[13] INTERNATIONAL STANDARD ISO/IEC 17799:2005
Iso-Iec 17799 2005.pdf
2005

[14] INTERNATIONAL STANDARD ISO/IEC 27001:2005
Iso Iec 27001 2005.pdf
2005

[15] INTERNATIONAL STANDARD ISO/IEC 27005:2008
Iso Iec 27005 2008.pdf
2008

[16] Barros, Oscar
Reingeniería de Procesos de Negocios
Editorial Dolmen, Chile, 1994
pp. 56

Tesis publicada con autorización del autor
No olvide citar esta tesis