Flumen (2): 5-734 (2015)
Revista de la Universidad Católica Santo Toribio de Mogrovejo
Chiclayo - Perú

Desarrollo de un SGSI para los Colegios Profesionales en la Región Lambayeque. Caso de estudio: Colegio de Ingenieros

Development of an ISMS for professional associations in the Lambayeque Region. Case Study: College of Engineering

César Augusto Córdova Oblitas[1]
(cacordova70@hotmail.com,
Gustavo Alfredo Morales Cueva[2]
gustavo_3587@hotmail.com,
José Antonio Samamé Martínez[3]
sama_pc@hotmail.com)

Resumen

Los colegios profesionales (CP) son instituciones autónomas con personería jurídica de derecho público interno, sin fines de lucro, creadas por ley, agrupan a los profesionales en el ámbito de su jurisdicción. La problemática radica en la falta de seguridad de la información (SI) en la organización, en la actualidad la información es un activo clave para las empresas, sin embargo no se resguarda de manera adecuada para cumplir con los objetivos estratégicos de la organización.

La información es parte principal en los procesos, servicios y tecnologías en el sector público o privado; sin importar el tamaño; es vital cumplir con las características de la SI: confidencialidad, integridad, disponibilidad (CID), en general se suele actuar de manera reactiva, desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI), permitirá actuar en forma proactiva ante eventos que afecten la SI. Se analizó enfoques de estándares para gestionar la SI (ISO 27000, COBIT, ITIL, MAGERIT).

Como objetivos de esta investigación culturizar a la alta dirección sobre SI, analizar las brechas, la identificación de los riesgos, identificar y evaluar los controles, y por ultimo plantear los proyectos de SI; finalmente se hace uso de la norma ISO 27001 en la aplicación al caso: Colegio de Ingenieros del Perú (CIP), implicó gestión de riesgos (GR), identificación de controles, normas, políticas y mejoras en los procesos de negocio definidos en el documento de alcance.

Palabras Clave: Gestión de riesgos, ISO/IEC 27000, SGSI, SI.

Abstract

Professional associations (CP) are autonomous institutions with legal personality under public law, nonprofit, created by law; bring together professionals in the field of jurisdiction. The problem lies in the lack of information security (SI) in the organization, now the information is a key asset for companies, though not adequately safeguards to meet the strategic objectives of the organization.

Information is principal and central part in processes, services and technologies in the public or private sector; regardless of size; is vital to meet the characteristics of the SI: confidentiality, integrity, availability (CID), the tendency is to act in a reactive way, develop a Management System Information Security (ISMS), allow to act proactively to events that affect the SI. It approaches standards were analyzed to manage the SI (ISO 27000, COBIT, ITIL, MAGERIT).

It was proposed as targets for this research culturizar to top management on SI, analyze gaps, identification of risks, identify and assess controls, and finally prepare draft SI finally use is made of ISO 27001 in the application to the case: Departmental Council of Lambayeque Engineers Association of Peru (CIP), involved risk management (GR), identification of controls, standards, policies and improvements in business processes defined in the scoping document.

Keywords: Risk Management, ISO / IEC 27000, ISMS, SI.

Recibido el: 05.01.2016
Aceptado el: 05.04.2016

Los investigadores son Ingenieros de Sistemas y Computación, egresados de la Universidad Católica Santo Toribio de Mogrovejo, grado de Magíster en Ingeniería de Sistemas y Computación con mención en Dirección Estratégica de TI.
[1] Ide Financial Service International, Senior Vice President and Executive Director of Information Security.
[2] Colegio de Ingenieros del Perú (Lambayeque), Encargado de TI.
[3] High Service International, Redes y Base de Datos.

Introducción

La dependencia en la tecnología de la información (TI), las regulaciones y requisitos de SI obligan a las empresas a evaluar procesos de negocio, datos de misión crítica, y apoyar el entorno de TI, entre otros. Lo mencionado anteriormente y con una baja inversión de TI que resulta en justificar cada compra, los profesionales de la seguridad se ven forzados a encontrar formas eficientes y eficaces para evaluar su organización cuyo fin es descubrir y priorizar el resolver vulnerabilidades, y para desarrollar soluciones rentables que muestren beneficio para el negocio.

Actualmente, el tema de SI a nivel internacional se toma de manera responsable por empresas e instituciones, que reconocen que la información es un activo fundamental para el negocio, con el fin de preservar y resguardar este activo, sin embargo en la mayoría de estas no está en sus planes resguardarla, desestimando su importancia o en algunos casos la Alta Dirección (o el Consejo Directivo) carece de conocimiento técnico-profesional con respecto al tema.

"La finalidad de la SI es proteger los recursos valiosos de la organización, tales como información, hardware y software. A través de la selección y aplicación de las salvaguardias adecuadas, la seguridad ayuda a una organización a cumplir sus objetivos de negocio o de su misión mediante la protección de sus recursos físicos y financieros, la reputación, la posición legal, empleados y otros activos tangibles e intangibles"[4].

El creciente interés sobre SI, ha conllevado a organizar congresos, reuniones de profesionales destacados sobre el tema, uno de estos el ESORICS[5] organizado en Inglaterra. En América se cuenta con ASIS[6] organizado en México, CIBSI y TIBETS[7], organizada por la Universidad Tecnológica de Panamá, estas organizaciones fomentan e imparten cursos y avances sobre la SI. En Perú, organizaciones como ISACA[8], entre otras, son encargadas de impartir conocimientos acerca del tema de Seguridad entre otros temas relacionados.

Abordar la problemática internacional sobre temas de SI conlleva a considerar diferentes perspectivas, algunas con una aportación crítica sobre otros, por lo cual se analizaron artículos y tesis de postgrado a nivel mundial; para conocer la situación actual y problemas relacionados con el tema en estudio, al final se obtuvo la conclusión después de estos análisis de los artículos y tesis, se procedió a entablar la relación con nuestro trabajo de investigación.

Si bien es cierto que los enfoques son distintos cada quien lleva la investigación por el camino que mejor le parece de acuerdo a hallazgos relacionados en cada investigación, en tal sentido las lecturas mencionadas en artículos y tesis los autores hacen referencia con énfasis la debilidad de la SI y la cual es el factor humano, en temas de importancia o relacionados al interés de la información.

A nivel local la problemática en el sector donde se desarrolló este trabajo fue en los Consejos Departamentales de los colegios profesionales (Contadores, Médicos, Ingenieros, Abogados, Arquitectos, Enfermeras, Psicólogos, Biólogos, etc.) de la región Lambayeque, la indagación sobre cuestiones de SI es un tema al cual se le ha restado importancia, no se cuenta con documentación de procesos, o aplicación de normas internas para el resguardo de la información de los colegiados, sin tener conciencia de los riesgos que tiene la organización.

El primer punto importante de la realidad encontrada, es que la mayoría de colegios no cuentan con un departamento de TI

4 Peltier, Information Security Fundamentals, xiii [traducida por los investigadores].
5 ESORICS (European Symposium on Research in Computer Security)
6 ASIS (Congreso Latinoamericano de Seguridad)
7 CIBSI y TIBETS (Congreso Iberoamericano de Seguridad Informática y Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información)
8 ISACA: Information Systems Audit and Control Association

propiamente dicho, algunos contratan empresas encargadas de velar por la TI, otros, solo cuando los equipos informáticos se dañan o se malogran, los llevan a reparar por cualquier técnico disponible en el mercado, lo que demuestra una cultura reactiva, no preventiva.

El segundo punto a tomar en cuenta, es que solo uno de los colegios cuenta con la información centralizada en un servidor y realiza respaldo de la información en días alternos, los demás colegios, tienen la información en alguna computadora, y cinco de ellos realizan respaldo de la información, pero no cuentan con procedimientos formales para realizarlo, simplemente se realiza y no hay un control (ver anexo 03).

Como tercer ítem a resaltar es que el uso de correos electrónicos es mediante servicios gratuitos (Gmail o Hotmail) en el cual los usuarios pueden acceder desde cualquier lugar, ya que cuentan con la contraseña y en algunos de ellos la información es enviada primordialmente por el correo electrónico. Otros puntos a considerar, es que se pueden utilizar dispositivos como laptops, dispositivos de almacenamiento externo, entre otros, para poder realizar el trabajo y no existe un control sobre la información almacenada en dicho equipo.

En el caso que cuenten con manuales de gestión, no son aplicados, e incluso en algunos casos cambian cuando ingresa otra directiva. La seguridad física no tiene la atención que debe, ya que en algunos casos no se cuenta con foto check o no existe un vigilante que controle el acceso, algunos col-egios no cuentan con cámaras de seguridad, solo uno ha contratado central de alarmas.

A nivel de organización, específicamente en el Colegio de Ingenieros del Perú Consejo Departamental Lambayeque, que es donde se realizó el caso de estudio, se han presentado diversas incidencias y problemas en los que la información ha sido expuesta, algunos de ellos se resumen a continuación: extravió de documentación de supervisiones de obras públicas, pérdida de certificados de cursos impartidos por el colegio, acceso a la sala de servidores por personas no autorizadas, acceso a la red inalámbrica sin clave de seguridad, acceso no restringido a las computadoras en los laboratorios, perdida de información contable por estropeo de disco duros, extravío de hardware de la organización, entre otros.

Los autores señalan como objetivo general el desarrollar un SGSI para los Consejos Departamentales de los colegios profesionales en la región Lambayeque, con un caso de estudio aplicado en el Colegio de Ingenieros. Y como objetivos específicos el determinar la documentación para culturizar a la alta dirección en SI, realizar el análisis de brechas, identificar los riesgos, identificar y proponer los controles, elaborar el plan de proyectos, todos estos de la SI. En este estudio al ser una investigación de nivel descriptivo, no requiere alcance de contrastación de hipótesis.

La metodología utilizada en el desarrollo de este trabajo es la propuesta por la norma seleccionada, la cual hace uso del ciclo de Deming o PDCA (Planificar, Hacer, Verificar y Actuar), y para la gestión de riesgos se utilizó la metodología propuesta por MAGERIT V3, así también se elaboró los documentos exigidos por la norma en la aplicación del caso de estudio. Como resultado se elaboró el desarrollo de la propuesta de un SGSI para los CP, con un caso de estudio aplicado en el CIP.

Un SGSI brinda la capacidad de reaccionar con rapidez ante cualquier incidente de SI. La ISO 27001 es exigida por los mercados internacionales a las empresas, para poder demostrar que la información que maneja está bajo características de la CID, y que garantizan continuidad en las operaciones, porque cuentan con un sistema para la planificación de la continuidad del negocio. Una empresa con la norma implantada garantiza, en la cadena de suministros, que es proveedor confiable.

En un enfoque centrado en los procesos para realizar evaluaciones, el elemento clave es la comprensión de objetivos, procesos de negocio, y cómo las medidas de seguridad, están alineadas con los riesgos del negocio. El diagnóstico realizado fue útil como base para la

construcción y el mantenimiento de un programa de SI. En el diagnóstico se incluyó un cuestionario que permitió llevar a cabo la evaluación de seguridad actual en el sector y también permitió entender la SI e identificar áreas de mejora.

Finalmente la implementación del SGSI permitirá tener la capacidad de reaccionar de manera proactiva ante cualquier incidente de SI. La falta de políticas y controles propios a la SI; conlleva a resultados que pueden afectar a los objetivos de la organización.

Marco teórico conceptual

Abordar la implementación y mantenimiento de un SGSI; conlleva a considerar diferentes perspectivas, algunas con un aportación crítica sobre otras. Esta sección tiene el propósito de conocer el estado del arte en esta área del conocimiento y se establecen las bases teóricas necesarias para investigar, interpretar y estructurar los modelos de SI. En primer lugar se analizaron artículos y posteriormente tesis de postgrado; para conocer la situación actual, problemas relacionados y finalizando con las conclusiones.

Se revisaron artículos que ayudaron en la investigación, tales como los siguientes:

Díaz, A., Collazos, G., et al (2012)[9], en su investigación denominada: *"Implementación de un SGSI en la comunidad Nuestra Señora de Gracia, alineado tecnológicamente con la norma ISO 27001".*

Como conclusiones de esta investigación se destaca que todas las organizaciones sin tener en cuenta su tamaño, implementen mecanismos que permitan mantenerla segura, implementar el SGSI resulta beneficioso para la comunidad en cuanto a seguridad efectiva en los IS, mejoras continuas en procesos de auditorías internas dentro de la comunidad, incremento de la confianza en la comunidad y mejora de su imagen.

Los autores Knappa, K., Morris, R., et al. (2009)[10]. Proponen en su investigación denominada: *"Política de seguridad de la información: un modelo de proceso a nivel organizacional"*, los resultados expusieron que existía necesidad de formación de los participantes para que el modelo funcione correctamente, una vez que las políticas sugeridas serían aprobadas, estas darían forma de la mejora al equipo, con una advertencia sobre el escándalo como el de Enron y la propuesta Ley Sarbanes-Oxley, resulta que requiere controles y contrapesos adicionales, mientras que la teoría es esencial, los autores señalan que la práctica determina la validez de la teoría.

Para Van Niekerk, J. y Von So*lms. R. (2009)[11], en su trabajo denominado: "Cultura de la seguridad de la información: una perspectiva de gestión"*, Refieren a la elasticidad en la cultura de la SI, la cual se define como la medida del cambio en una variable, se puede hacer si la empresa cuenta con los medios para efectuar el cambio. A esto se une el consentimiento de la gestión de la seguridad; es decir, si es exigente con los empleados en el cumplimiento y lo que es el mínimo de la línea de base de seguridad; aceptable para realizar el trabajo. Una fuerte cultura de la SI es interpretada como una cultura deseable que sea conducente y estable, lo mejor de la cultura de SI es la que se puede predecir.

Fuchs, L., Pernul, G. y Sandhu, R. (2011)[12], en su investigación denominada: *"Roles en seguridad de información: una encuesta y clasificación del área de investigación"*, La

9 Díaz Andrés, et al "Implementación de un Sistema De Gestión De Seguridad De La Información (SGSI) en la Comunidad Nuestra Señora de Gracia, alineado tecnológicamente con La Norma ISO 27001". (2012).
10 Knappa, Kenneth, Morris, Franklin, et al. "Information security policy: An organizational-level process model", computers & security, USA. (2009).
11 Van Niekerk, Johan y Von Solms, Rossouw. "Information security culture: A management perspective", computers & security, South Africa. (2009).
12 L. Fuchs, G. Pernul, R. Sandhu (2011). Roles in information security - A survey and classification of the research area, Alemania.

metodología, consiste en cuatro pasos principales: selección de bibliografía, consulta de búsqueda, revisión de resultados, y la extensión de los resultados, se clasificaron utilizando un enfoque de agrupación de tres niveles jerárquicos, el áreas de investigación se dedicó a dos grupos: la clasificación de los resultados y la definición de la clasificación, esto llevó a la determinación del valor de cada documento de modelos a seguir (elemento fundamental de un sistema de roles) y administración, rol que incluye la descentralización de la competencia, la autonomía administrativa, y el control de las irregularidades.

En su investigación Ashenden, D. (2008)[13], denominada; *"Gestión de seguridad de la información: ¿es un desafío humano?"*, El desafío humano ha sido definido como la gestión de las personas en una organización, dentro de sus funciones específicas, pero a la vez reconoce que tienen identidad personal y social que influyen en su comportamiento. Este artículo aborda la gestión de la SI desde un tema cultural, indica la importancia que la persona este comprometida en aceptar, procesar, transmitir e implementar una SI en toda la organización, para lograr una configuración óptima de los recursos a fin de cumplir con los objetivos del negocio.

Por su parte Ormella, C. (2014)[14], en su trabajo denominado: *"Gobierno de seguridad de la información"*. Proteger la reputación de la organización, mejorar la confianza en las relaciones con los clientes, posibilitar nuevas y mejores formas para procesar las transacciones electrónicas, el objetivo del Gobierno de SI es que alcance los siguientes resultados básicos de un gobierno eficaz de seguridad como: la alineación estratégica, administrar los riesgos, entregar valor, administración de recursos, medición del desempeño, integración.

Santos-Olmo A., Sánchez L., et al (2011)[15], en su estudio: *"Características deseadas para un SGSI orientado a pequeñas y medianas empresas (PYMEs)"*, concluyen y demuestran, que la mayoría de los modelos de gestión de seguridad se han basado en el estándar internacional ISO/IEC17799 y los más exitosos en grandes empresas son la ISO/IEC27001, COBIT y ISM3, como resultado de esta investigación, se ha podido obtener un conjunto de características que un SGSI orientado a PYMEs debe tener y cómo podemos enfrentar cada una de estas características utilizando diferentes componentes de los estándares e investigaciones más relevantes hoy en día.

Por otro lado Spremic, M. y Popovic, M. (2008)[16], en su investigación *"Problemas emergentes en el gobierno de TI: implementación del modelo de gestión de riesgos de TI corporativo"*, el problema de la GR de TI se convierte cada vez menos en un problema técnico, y cada vez más en "problema empresarial", muchas compañías nombran a directores ejecutivos para estas actividades, el Modelo Corporativo de GR de TI incorpora gobierno y auditoría de TI, los planes para investigaciones a futuro incluyen pruebas del modelo corporativo de GR de TI en un amplio rango de empresas de varias industrias. Las dificultades pueden surgir por las empresas en general no desean participar en tales investigaciones, porque pueden revelar algunas vulnerabilidades en sus negocios y exponerlas a cierto riesgo.

Después del análisis de los artículos y tesis se procedió a establecer la relación con esta investigación, las lecturas relacionadas en artículos los autores mencionan con énfasis la debilidad de todos los SGSI y la cual es el factor humano. La preocupación de los trabajos realizados y analizados se ha visto relacionada a crear nuevas metodologías para los SGSI, en este trabajo se aterrizar el enfoque de las investigaciones analizadas.

13 Ashenden, Debi. "Information Security management: A human challenge?, Reino Unido. (2008)
14 Ormella Carlos. "Gobierno De La Seguridad De La Información", Argentina. (2014).
15 Santos-Olmo, Antonio, Sánchez, Luis, Fernández-Medina, Eduardo, Piattini, Mario. "Desirable Characteristics for an ISMS Oriented to SMEs", China. (2011)
16 Spremic, Mario y Popovic, Matija. "Emerging issues in IT governance: implementing the corporate IT risks management model", USA. (2008).

Materiales y Métodos

Se hace uso de entrevistas, análisis y observación. Las entrevistas se apoyaron en técnicas como el cuestionario y comunicación abierta, para poder obtener la información de los colegios profesionales, se realizó la visita de los mismos en dos ocasiones, la primera con la participación de ocho Colegios profesionales (contadores, médicos, ingenieros, abogados, arquitectos, enfermeras, psicólogos y biólogos) con un cuadro de verificación que permitió a los investigadores conocer la realidad a priori; luego de ahondar en el estudio se realizó un cuestionario con base en la norma ISO 27001, enfocándonos en las dimensiones del estudio, en la cual participaron los colegios profesionales antes mencionados, agregando a químicos farmacéuticos, administradores y obstetras, aportar con nuestra investigación. El análisis, aplicado al caso de estudio en el CIP, apoyado en documentación histórica, que abarca los procesos críticos, los incidentes de seguridad de información, las funciones más importantes, la misión y visión del CIP, entre otros. La observación, de gran utilidad para conocer la realidad tecnológica, los procesos de TI y la seguridad de la información.

Resultados

En este punto se realizó una descripción y análisis de las fases desarrolladas del SGSI en el CIP. Se ha considerado un cierto número de controles a implementar en la SI de acuerdo a los procesos que se determinaron en el presente estudio, y culturizar en temas de SI, teniendo en cuenta la protección de los datos y la privacidad de la información personal, protección de los registros de la información, derechos de la propiedad intelectual, documentación de la política de SI, asignación de responsabilidades.

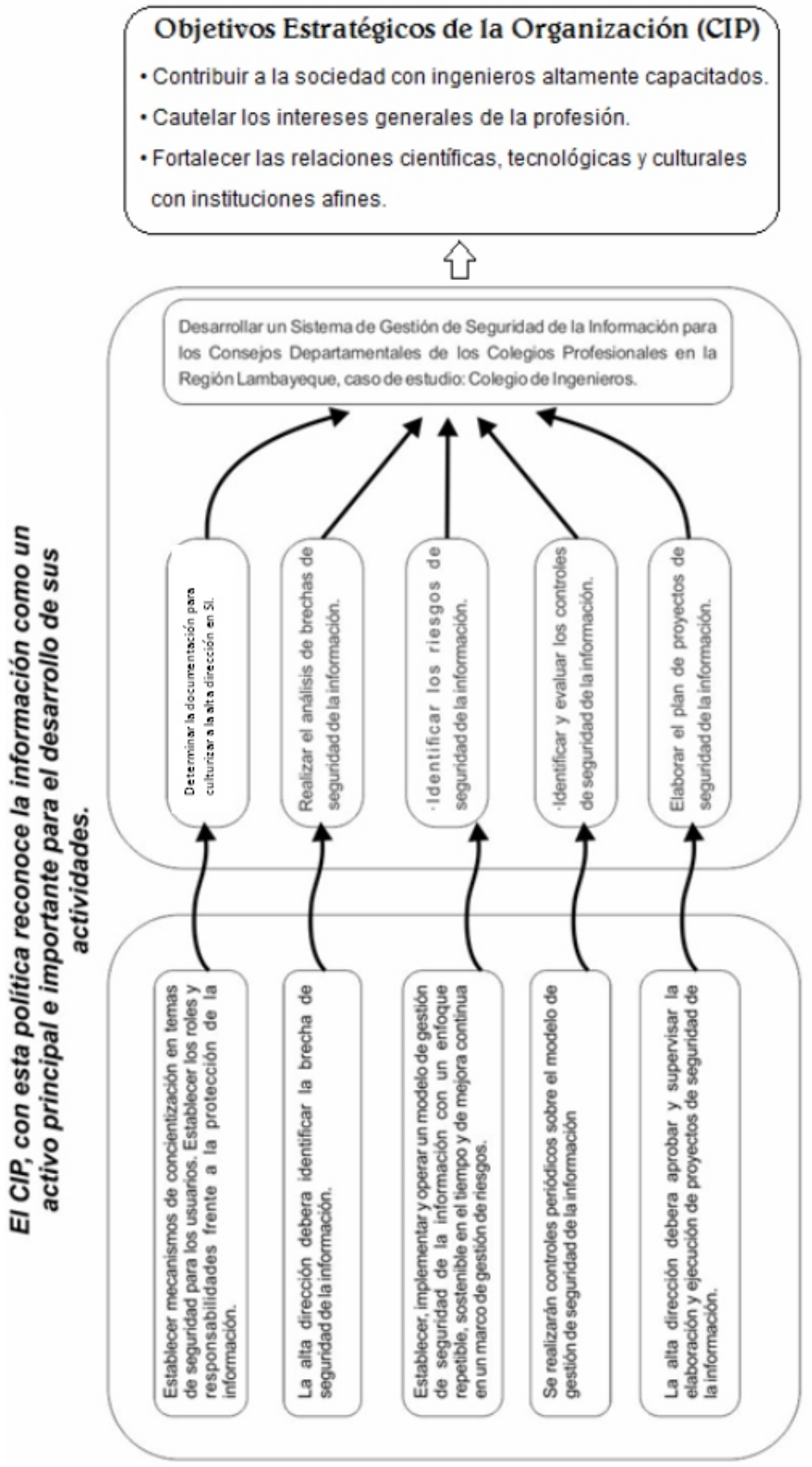
Por otro lado y de acuerdo al alcance de nuestro SGSI se identificó a los stakeholders, como el Decano, Contador, Asistente contable, Encargada de Colegiatura, Coordinador de capacitaciones, Encargado de sistemas, Encargado de soporte, Secretaria, Equipo de proyecto de investigación.

Política general

En cumplimiento con la norma ISO 27001 en el numeral 5.2, cuyo propósito es definir el objetivo, dirección, principios y reglas básicas para la gestión de la SI, se elaboró la política que se aplica al CIP, documento que se encuentra en el trabajo de tesis como parte de los entregables de la norma, en el gráfico 01, se puede apreciar la correlación entre objetivos y políticas establecidas en el SGSI.

Se elabora un gráfico para establecer la correlación entre políticas, objetivos establecidos y objetivos del negocio.

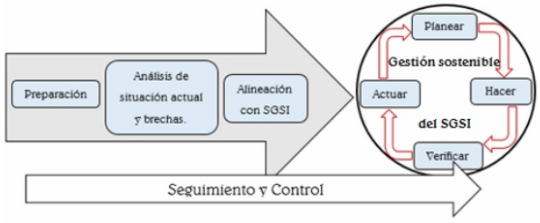
Gráfico : Evaluación de políticas con objetivos del negocio



Fases del ciclo de Deming o PDCA

Se aplicó la metodología propuesta por ISO 27001, la cual se desarrolla en cuatro (4) fases del ciclo de Deming o PDCA (Plan - Do - Check - Act) que nos permitirá, hacer una mejora continua de las fases que son necesarias a fin de llevar a cabo la implementación del SGSI.

Gráfico 2: Plan de implementación de SGSI.



FUENTE: Centro de Investigación de Telecomunicaciones 2011 - Modelo de SI.

Posteriormente de elaboro el desarrollo de las cuatro fases que componen el ciclo Deming, dando cumplimiento al desarrollo del SGSI propuesto para el CIP.

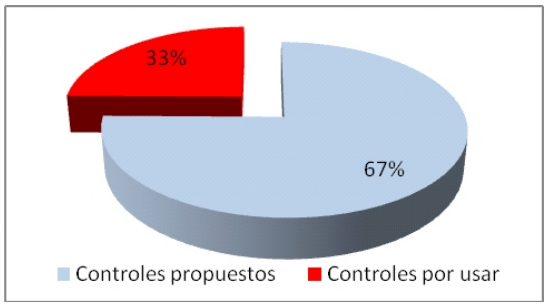
Controles utilizados de la ISO 27001, por dominios definidos en el alcance

Realizado el estudio y determinando los controles establecidos por la norma en base a las dimensiones y procesos establecidos y acordados con la Alta Dirección del CIP, se estableció los siguientes Dominios y sus controles, en los siguientes gráficos se aprecia los controles propuestos implementados y los controles por implementar.

Controles del dominio de la cultura organizacional

El siguiente gráfico muestra que del 100% de los controles propuestos en este dominio, se ha utilizado el 67%, faltando por implementar un 33%. Lo que nos permitirá mejorar en este dominio, es muy importante reconocer que la implementación de estos controles no nos asegura una buena cultura organizacional si es que no se hace seguimiento de su ejecución, aplicación y mantenimiento por parte de los responsables.

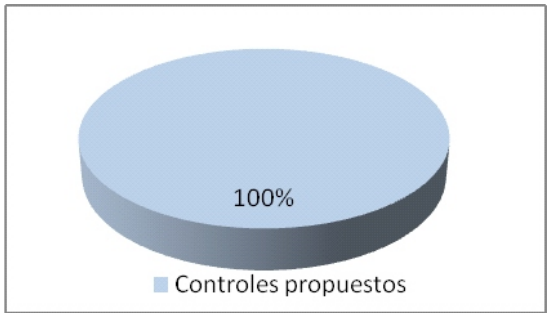
Gráfico 3: Controles de cultura organizacional



Controles del dominio de la seguridad de los recursos humanos

Tal como se muestra en la gráfica siguiente la implementación a un 100% de los controles propuestos, pero cabe asentar que el 100% de controles implementados no asegura nada, ya que esto siempre debe estar en constante revisión por los responsables.

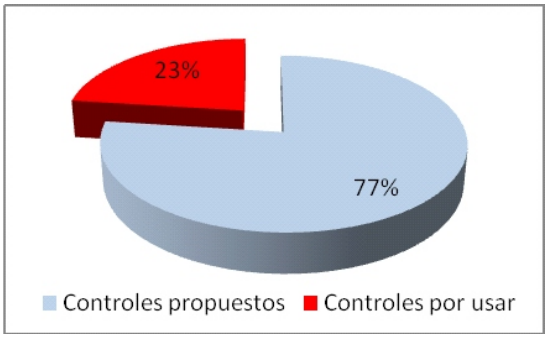
Gráfico 4: Controles de seguridad de los recursos humanos



Controles del dominio de Seguridad Física y Ambiental

En el siguiente gráfico se puede apreciar que del 100% de los controles propuestos, se ha utilizado el 77%, faltando por implementar un 23%, lo que nos permitirá obtener una buena seguridad de nuestras instalaciones, aunque esto no significa que la protección está asegurada al 100%, por lo que hay que seguir monitoreando nuestro sistema.

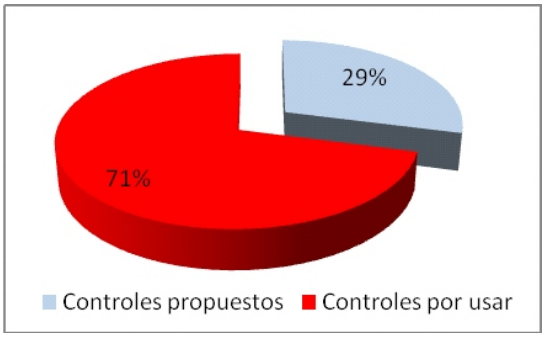
Gráfico 5: Controles de seguridad física y ambiental



Controles del dominio de gestión de incidencias de SI

La observación en el siguiente grafico se aprecia que del 100% de los controles propuestos, se ha utilizado solo el 29%, faltando por implementar un 71%, conforme se vaya implicando los empleados con el sistema estos controles se irán implementando a medida de cumplir con su totalidad.

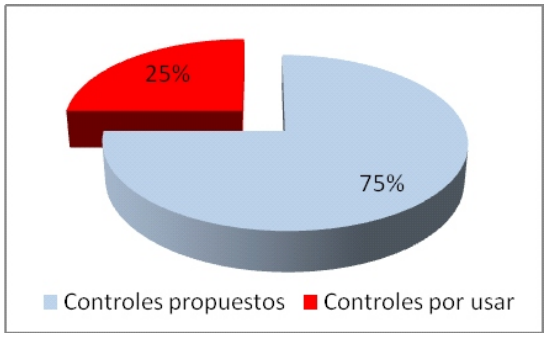
Gráfico 6: Gestión de incidencias de SI



Controles del dominio de gestión de la continuidad del negocio en SI

El gráfico muestra que del 100% de los controles propuestos, se ha utilizado el 75%, faltando implementar un 25%, es un buen índice de controles implementados, pero a medida que el personal se involucre con el SGSI se recomienda la implementación gradual de controles.

Gráfico 7: Gestión de la continuidad del negocio en SI



Lista de entregables exigidos por la norma ISO 27001

Los entregables que forman parte del desarrollo del SGSI son:

SGSICIP01 - Evaluación de la situación de seguridad actual (línea de base).docx

SGSICIP02 - Análisis de brechas.xlsx

SGSICIP03 - Definición del alcance del SGSI - cip.docx

SGSICIP04 - Políticas del SGSI - cip.docx

SGSICIP05 - Declaración de aplicabilidad.docx

SGSICIP06 - Cronograma - propuesta de solución.xlsx

SGSICIP07 - Diagrama de dependencias.png

SGSICIP08 - Procesamiento de las encuestas.xlsx

SGSICIP09 - Evaluación de riesgos.xlsx

SGSICIP010 - Plan de tratamiento del riesgo.xlsx

Conclusión

La implementación del SGSI nos permitirá asegurar que podemos actuar de una manera asertiva y proactiva; para tener la capacidad de reaccionar con rapidez ante cualquier incidente de SI. Es importante que todos los miembros de la organización deban tomar las medidas de protección necesarias para la información; porque está siempre expuesta a amenazas.

La falta de políticas y controles propios a la SI; conlleva a resultados que pueden afectar a los objetivos de la organización, la alta dirección y todos los miembros de la organización deben involucrarse, con responsabilidad en el cumplimiento de políticas, normas y controles de la organización. El SGSI debe verse como el camino para ayudar al cumplimiento de los objetivos institucionales.

El cumplimiento a nuestros objetivos propuestos en esta tesis se obtienen por el estudio realizado en el sector de los colegios profesionales de la región Lambayeque donde se determinó a situación actual en que se encuentran con respecto a temas de SI, la implementación del SGSI utilizando la norma ISO/IEC27001:2013, nos sirvió como una herramienta eficaz para este logro.

En cuanto a nuestro primer objetivo específico (OE) como determinar la documentación para culturizar a la alta dirección en SI, se sostuvo reuniones con la alta dirección para obtener la aprobación y el respaldo de los principales colaboradores durante el desarrollo del SGSI en el CIP, por lo cual se firmó una carta de autorización y respaldo para definir el alcance del proyecto, asimismo documentación que respalda el desarrollo del SGSI.

Se realizó el análisis de brechas cumpliendo nuestro segundo OE, con la finalidad de determinar, en las dimensiones de investigación cuáles son los controles, según la ISO 27001, que se cumplen, no se cumplen y se cumplen parcialmente en el CIP. Del total de los controles que aplican (treinta y seis) el 86.11% no se cumplen y el 13.89% se cumplen parcialmente, lo que evidencia que la mayoría de controles no están siendo cumplidos en el CIP.

En nuestro tercer OE se identificaron los riesgos de SI que afectan a los principales activos en la institución, para ello se realizó la evaluación de riesgos utilizando la metodología MAGERIT; se caracterizó todos los activos del CIP, valorizando cada uno según CID, identificando vulnerabilidades, amenazas y riesgos de dichos activos; luego en base al impacto y la probabilidad se obtuvo el riesgo inherente y finalmente las salvaguardas o controles con la respuesta al riesgo y el indicador del riesgo.

Como cuarto objetivo específico se identificó los controles en base a los riesgos identificados con el objetivo de mitigar, evitar, transferir o aceptar el riesgo.

Cumpliendo nuestro último OE se elaboró la cartera de proyectos de SI (veintisiete) considerando los recursos y los responsables de cada uno de ellos, en base a los controles aplicados en el estudio y establecidos por las ISO/IEC27001:2013 lo cual permitirá tener un equilibrio en el SGSI.

Por otro lado y como complemento a esa propuesta se recomienda la implementación de un sistema de SGSI valiéndose de alguna herramienta que permita la automatización, así como la elaboración de un cuadro de mando integral (BSC) que permitirá la mejora continua del SGSI.

Agradecimiento

Expresar gratitud, hacia todos los CP, que nos abrieron las puertas y nos permitieron la investigación, sin su apoyo y soporte, no hubiera sido posible seguir adelante, un agradecimiento especial al Ing. Ciro Antonio Salazar Montaño, Dr. Alfonso Salvador Díaz Gálvez, y por la generosidad y paciencia con nuestro asesor el Mgtr. Juan Dávila Ramírez, así como al apoyo incondicional del Ing. Héctor Zelada Valdivieso, al Mgtr. Pedro Jacinto Mejía, a nuestras familias amigos y colegas.

Referencias Bibliográficas

Ashenden, Debi. Information Security management: A human challenge?, Reino Unido. (2008)

Díaz Andrés, Gloria Collazos, Hermes Cortez, Leidy Ortiz, Gustavo Herazo Pérez. Implementación de un Sistema De Gestión De Seguridad De La Información (SGSI) en la Comunidad Nuestra Señora De Gracia, alineado tecnológicamente con La Norma ISO 27001. (2012).

ISO/IEC 27001:2013 Tecnología de Información. Técnicas de Seguridad. Requerimientos de Sistema de Gestión de Seguridad de Información.

Kenneth J. Knapp, R. Franklin Morris Jr., Thomas E. Marshall, Terry Anthony Byrd. Information security policy: An organizational-level process model, computers & security, USA. (2009).

L. Fuchs, G. Pernul, R. Sandhu. Roles in information security - A survey and classification of the research area", Alemania. (2011).

Ormella Carlos. Gobierno De La Seguridad De La Información, Argentina. (2014).

Peltier, Thomas. Information Security Fundamentals, EE.UU. (2014).

Santos-Olmo, Antonio, Sánchez, Luis, Fernández-Medina, Eduardo, Piattini, Mario. Desirable Characteristics for an ISMS Oriented to SMEs, China. (2011)

Spremic, Mario y Popovic, Matija. Emerging issues in IT governance: implementing the corporate IT risks management model, USA. (2008)

Van Niekerk, Johan y Von Solms, Rossouw. Information security culture: A management perspective, computers & security, South Africa. (2009).