¿POR QUÉ FRACASAN LOS PROYECTOS DE SEGURIDAD DE LA INFORMACIÓN?

Luis Antonio Tristancho Robles
Universidad Piloto de Colombia
trobles.luis@gmail.com

Abstract **- The lack of knowledge and experience of the staff that designs and implements the Information Security Management System (ISMS), the indifference of management and/or directors of the company, a project without formal structure, the lack of roles and responsibilities, the high cost, the apathy of the Organization's staff and of course the ignorance of the laws and regulations are among other factors that define the success of ISMS. This article describes a number critical factors that affect the Pareto of the implementation of the ISMS in an organization.**

Resumen **- La falta de conocimiento y de experiencia del personal que diseña e implementa el Sistema de Gestión de Seguridad de la Información (SGSI), la indiferencia de la gerencia y/o directivos de la empresa, un proyecto sin estructura formal, la falta de roles y responsabilidades, el elevado costo, la apatía del personal de la organización y por supuesto el desconocimiento de las leyes y regulaciones, son entre otras las causas que definen el éxito del SGSI. Este artículo describe una serie factores críticos que inciden en el Pareto de la implementación del SGSI en una organización.**

Palabras Clave: Proyecto, Alta Dirección, Roles y responsabilidades, seguridad informática.

I INTRODUCCIÓN

En la actual comunidad global, donde gran parte de la información viaja a través del ciberespacio expuesta a una serie de vectores de ataque, que van desde las ciber amenazas hasta el conflicto de intereses e incumplimiento de regulaciones, surge el concepto de SGSI (Sistema de Gestión de Seguridad de la Información) como una fórmula magnífica para la protección de la información. No obstante, ponerla en práctica requiere de acciones y actividades que en gran parte de los casos resultan infructuosos o difíciles de mantener.

No hace más de una o dos décadas que las organizaciones no tenían estas preocupaciones o solo les inquietaban algunos programas maliciosos, hoy en día cuando el nivel de transacciones electrónicas que viajan a través de las redes de datos se mide en el orden de TERA y PETA bytes y que la información contenida es de gran valor, re aparece la piratería, pero esta vez en el ámbito cibernético. Entonces se debe pensar, qué tanto se está expuesto a este grupo delincuencial y si la información que se produce es objeto de un ataque o existe algún tipo de interés para un tercero, creer lo contrario es uno de los errores más comunes en seguridad – "esto no me toca".

Si buscamos en Google "Seguridad de la información" seguramente encontramos más 25 millones de resultados y muchos de estos resultados hacen referencia a equipos, software metodologías, consultorías, normas, etc., que prometen la solución a todos los problemas, no obstante, estas soluciones por si solas logran proteger tan solo una parte de los activos, en tanto que la combinación y su personalización, permitirán obtener buenos resultados en materia de seguridad.

No hay sistema ni organización 100% segura, un firewall no puede detener un atacante interno y una norma o política no detiene un atacante externo, pero si a estos se les une una estricta gestión de riesgos, un buen grado de concienciación y un excelente clima laboral, los resultados serán extraordinarios. Adicionalmente y como lo afirma, J.M San Martin en [1], la mayoría de los sistemas informáticos implantados en las empresas no son seguros, bien porque no fueron diseñados para ser seguros, bien porque no cuentan con los medios técnicos necesarios.

Finalmente, continua J.M San Martin en [1], "la Seguridad no se consigue solo con medios técnicos. Para lograr un adecuado nivel de Seguridad en la empresa, es fundamental disponer de una gestión y unos procedimientos adecuados, mediante los cuales se planifiquen los sistemas de protección y control necesarios. En definitiva, se necesita implantar un Sistema de Gestión de Seguridad que abarque y tenga en cuenta a toda la organización, desde sus directivos y empleados, a sus clientes, proveedores, e incluso accionistas, así como sus procesos y recursos productivos."

II MOTIVOS QUE ARRUINAN LOS PROYECTOS DE SEGURIDAD DE LA INFORMACIÓN

Existen algunas consideraciones arraigadas sobre todo en esferas administrativas y gerenciales que frenan el ciclo de vida y desempeño de un Sistema de Gestión de Seguridad de la Información (SGSI). Estos vicios conllevan a menudo si no al fracaso en la implementación, por lo menos imprimen altos costos al proyecto haciéndolo inviable y poco atractivo.

No cometer estos errores o sortearlos adecuadamente, permitirán no solo que la implementación sea exitosa, sino más fácil y que efectivamente se vean los resultados esperados y al costo adecuado.

A. **Mala concepción**

No es lo Mismo Seguridad de la Información (SI) que gestión de la Tecnología de la Información (TI).

En muchas empresas y en particular aquellas que aún no tienen conciencia de la importancia o el valor de la información, se sigue pensando que la seguridad de la

información y la Tecnología de la Información son sinónimos, y que solo se trata de computadores. Si bien es cierto, gestionar la seguridad de la Tecnología de la Información es de gran importancia en el contexto general de la seguridad de la información, también existen otros aspectos muy importantes relacionados con asuntos organizacionales que generalmente están fuera del alcance de la gestión de TI.

La TI por sí sola no presenta un riesgo, es la conducta humana la que lo genera, es posible contar con buenas medidas de seguridad en TI, pero un administrador del sistema (descontento o un error involuntario) puede ocasionar un daño, sin que esto se constituya en un problema de computadores, más bien tiene que ver con procesos, personas, control, entre otros.

Según Dejan Kosutic, en [2], el anexo A de la ISO 27001 brinda 114 controles que están distribuidos de la siguiente manera:

Tabla I
RELACIÓN DE CONTROLES ISO 27001

IT related controls	37%
controls related to organization / documentation	36%
Physical security controls	13%
Legal protection controls	4%
Controls related to relationship with suppliers and buyers	5%
Human resources management controls	5%

Information security or IT security? Dejan Kosutic. (Nov 2014). En [2]

Como se puede observar, menos del 40% de los controles son atribuibles a TI, por lo tanto pensar que la seguridad de la información es lo mismo que gestión de la tecnología de la información es un error que deteriora la comprensión y el alcance del proyecto al no incluir los demás componentes.

De acuerdo con Dejan Kosutic en [2], la seguridad de la Información debe ser vista como un proyecto para toda la empresa, donde las personas relevantes de todas las unidades de negocio deben tomar parte, la alta dirección, el personal de TI, expertos legales, gerentes de recursos humanos, personal de seguridad física, la parte comercial de la organización, etc. Sin tal enfoque se terminará trabajando en la seguridad de TI, y eso no protegerá a la organización de los mayores riesgos.

B. **No se tuvo el respaldo de la alta dirección**

En un proyecto que finaliza de manera anormal, generalmente se puede escuchar: "No había quien tomara decisiones complejas", "el proyecto solo le interesaba a una persona", "Esa empresa es de nadie" y así sucesivamente una serie de frases que demuestran una condición de apatía y la falta de compromiso de la alta dirección, dejando como resultado el abandono del proyecto.

Como en cualquier otro proyecto, si no se asegura los recursos financieros, técnicos, logísticos y humanos necesarios, fracasará. Por lo tanto, la única forma de obtener esos recursos es haciendo que la dirección acepte el proyecto.

Así las cosas, es importante preguntar: ¿Cómo venderle el proyecto a la gerencia?, ¿Cómo lograr que se interese?, y la clave está en mostrar los beneficios que traerá el proyecto, no solo en materia de seguridad de la información, sino en el ámbito financiero, legal y humano. A continuación se expone la estrategia para justificar el proyecto a la alta dirección.

- *Reducción de costos:* En este aspecto la Seguridad de la Información ofrece grandes ventajas dado su principio de prevención, "la inversión actual es ahorro futuro", si se logra prevenir un incidente de seguridad, se ahorra el costo de los daños que podría ocasionar. No obstante convencer a la gerencia que vale la pena invertir en seguridad es una tarea difícil y precisa calcular el costo de las consecuencias en caso de que ocurra un incidente.

Christian Locher, en [3] "Methodologies for evaluating information security investments, 2005", define el término (ROSI), del inglés Return On Security Investment, Retorno Sobre la Inversión de Seguridad como:

$$\text{ROSI} = \text{monetary risk mitigation} - \text{cost of control} \quad (1)$$

De acuerdo la formula anterior, se determina que una inversión en seguridad es rentable si el efecto de mitigación del riesgo es mayor que los costos estimados del control. Para poder determinar estos valores, es necesario realizar una valoración juiciosa de los riesgos, determinando la probabilidad de ocurrencia, el costo aproximado del daño y el costo de las contramedidas y/o controles de seguridad.

Por ejemplo: para mitigar el riesgo de daño de un sistema de almacenamiento de un servidor se necesitan 90 millones de pesos incluyendo todos los costos para dejarlo tal como estaba en el momento del incidente, las estadísticas muestran que la probabilidad que esto ocurra es de 1 cada 20 años. Entonces la Mitigación del Riesgo mes (MRm) será:

$$\text{MRm} = (90.000.000 / 20) / 12 = 375.000 \quad (2)$$

Lo que significa que mientras la inversión en sistemas de respaldo sea menor a $375.000 por mes, se obtendrá una ganancia.

Como se mencionó anteriormente no es tarea fácil y en muchas ocasiones se tendrá que echar mano a la experiencia del personal que implementa para no incurrir en cifras incoherentes.

- *Cumplimiento legal*: Con todo el paquete normativo que en la actualidad generan los gobiernos en materia de seguridad de la información, de delitos informáticos, de protección de datos, etc., es evidente que la importancia en el cumplimiento de la normatividad defiende por si sola al proyecto, la certeza de que se está cumpliendo y no está incurso algún tipo de sanción que genere multas, es el principal beneficio del proyecto.
- *Optimización de los procesos*: Es probable que las empresas que tienen informalidad en sus procesos, tengan mayores riesgos de seguridad, al no definir de manera correcta los roles de cada uno de los empleados y directivos. Lo anterior da como resultado un desperdicio de recursos y de tiempo.

Con una definición clara de procedimientos, la seguridad estará presente a lo largo y ancho de la organización, con procedimientos seguros los riesgos se reducen disminuyendo el costo de controles, este es otro de los beneficios inmersos en la optimización de los procesos.

- *Ventaja competitiva*: La protección de datos personales, la propiedad intelectual, los controles de tipo legislativo y organizativo y la salvaguarda de registros

esenciales de la empresa son entre otras, las razones que demuestran un tratamiento seguro de la información.

Una organización que posee estas características obtiene de inmediato la confianza de sus clientes, proveedores y empleados, contribuyendo al mejoramiento de la imagen y por consiguiente la diferenciación ante la competencia. Esta diferenciación es una herramienta de venta que permite acercarse a nuevos clientes y por supuesto retener los existentes. Según J.M, San Martin, en [1] "Se puede afirmar que aquellas empresas que protegen la Información de forma adecuada disponen de una ventaja competitiva clara frente a otras que no lo hacen."

C. No se establece una estructura formal del proyecto

Si bien SGSI es un proceso sistemático, su implementación es un esfuerzo de una sola vez, lo que concuerda con la definición de proyecto en [4] según el (PMBOK) Project Management Body of Knowledge "es un esfuerzo que se lleva a cabo para crear un producto, servicio o resultado único, y tiene la característica de ser naturalmente temporal, es decir, que tiene un inicio y un final establecidos, y que el final se alcanza cuando se logran los objetivos del proyecto o cuando se termina el proyecto porque sus objetivos no se cumplirán o no pueden ser cumplidos, o cuando ya no existe la necesidad que dio origen al proyecto".

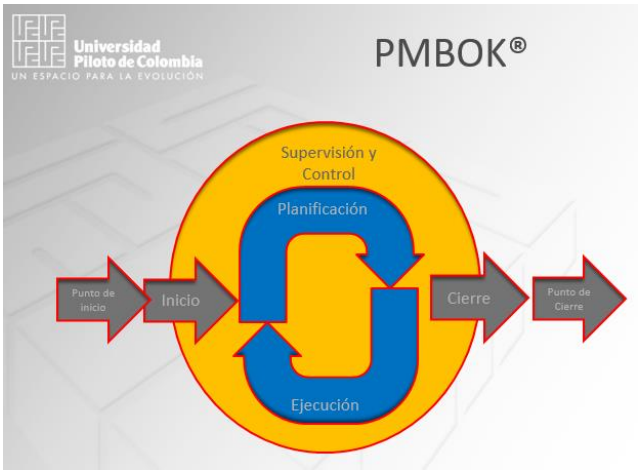

Fig. 1. Unipiloto, DiplomadoUPC_Gerencia_Unidad1.pptx, Página 8, Octubre de 2014. Unipiloto Imagen tomada de DiplomadoUPC_Gerencia_Unidad1.pptx (Fecha de actualización: 7 de Octubre de 2014)

Es posible evaluar en la anterior figura, que la ejecución de un proyecto conlleva una serie de pasos y recursos los cuales deberán ser ejecutados en su totalidad y así lograr el objetivo.

Todo proyecto por pequeño que sea y sin importar el marco referencial o la metodología utilizada requiere de un gran esfuerzo, el trabajo de planeación, ejecución, supervisión y control de implementación es algo muy complejo que debe ser abordado por un equipo de trabajo formalmente estructurado, no obstante en numerosas organizaciones, solo una o dos personas son las encargadas de realizar la totalidad de los trabajos. Es imposible que alguien resulte haciendo la implementación como un trabajo secundario, sin plazos, responsabilidades ni objetivos definidos y que al final se obtengan buenos resultados. Entonces es primordial que la implementación de la seguridad de la información, sea tratado como un proyecto mínimamente de medianas proporciones, dada su naturaleza de cambio cultural.

Algunas recomendaciones a tener en cuenta en la planeación y ejecución de este tipo de proyectos son:

1. *Prepárese para el proyecto*: Tomar conciencia de que se acercan arduas jornadas de trabajo, que hay cambios y que surgirán conflictos laborales y personales que deberán ser resueltos, es un buen punto de partida. Una buena preparación influye en los resultados del proyecto.
2. *Planee los recursos*: Se debe definir un organigrama del proyecto que contenga los recursos financieros, técnicos y humanos, al igual que la definición de roles y responsabilidades. Cuando se trabaje en el cronograma del proyecto, tenga en cuenta que el exceso en los tiempos de implantación no solamente genera sobre costo, sino también desmotivación y desinterés en el personal, finalmente es recomendable dividir el proyecto en fases dependiendo del tamaño y el alcance, pero siempre deberá ser mirado en conjunto.
3. *Defina hitos*: Los hitos dentro del proyecto son una señal de que se ha llegado a un punto importante, por ejemplo para una fecha determinada se tendrá el inventario de activos o el 50 % del proyecto estará listo al terminar la valoración de riesgos. Estos pequeños pasos o alcanzables ayudaran a mantener el control del proyecto y sirven como herramienta de comunicación para las partes interesadas.
4. *Comunique los avances:* Dedicar a diario un periodo corto de tiempo para evaluar resultados y aplicar correctivos evita tratar de remediar grandes problemas; de igual manera echar un vistazo rápido a las próximas actividades, previene y reduce al mínimo lo inadvertido. Semanalmente se debe realizar una reunión con el equipo de trabajo para evaluar lo conseguido hasta ahora y fijar acciones que permitan hacer los ajustes pertinentes. Estas reuniones deben ser efectivas, es decir:
   - *Programadas*: Los participantes de antemano saben de lo que se va a hablar.
   - *Proactivas*: Las críticas solo son aceptadas para sumar y construir, si hay que llamar la atención sobre algo, debe hacerse de manera proactiva.
   - *Cortas*: 30 a 45 minutos no refrigerio y lenguaje claro.
   - *Objetivas*: Los participantes deben tener claro sus responsabilidades para los próximos días.

   Con una periodicidad no tan alta debe informarse a la alta gerencia y a las partes interesadas sobre lo que está ocurriendo en el proyecto, avances, dificultades encontradas y como fueron resueltas, evitando un lenguaje técnico. Este informe puede hacerse de manera escrita o en reunión muy corta y desde luego teniendo en cuenta los principios de las reuniones efectivas.
5. *Especifique entregables*: Es preciso definir los resultados esperados. Por ejemplo, alcance, diagnóstico de brecha, activos de información, matriz de riesgos, plan de tratamiento, procedimientos, controles, entre otros.
6. *Haga una pausa*: Como se dijo en el numeral uno de este capítulo, el trabajo en la implementación del proyecto de Seguridad de la Información es arduo, las dificultades desgastan y cansan, por consiguiente es importante evitar que el equipo de trabajo y el personal involucrado tengan un

debilitamiento excesivo, provocando bajo rendimiento, retrasos y dilatación de actividades.

En lo posible se recomienda un tiempo dedicado al entretenimiento, totalmente diferente a la rutina del día a día, en donde el grupo realice actividades lúdicas y que no tengan nada que ver con el proyecto.

D. **No se cuenta con la experiencia suficiente**

Fig. 2. Consultor virtual gratuito para ISO 27001 e ISO 22301, EPPS Services Ltd 2015. Imagen tomada de http://www.iso27001standard.com/es/

La figura anterior muestra un esquema macro para la implementación de un SGSI de acuerdo con la norma ISO 27001. Es posible observar que se debe contemplar algunas opciones, desde hágalo usted mismo, hasta la asistencia y asesoramiento de un especialista. Según Dejan Kosutic en [5], no importa el marco referencial o la norma que haya seleccionado, este no le otorgará todo el conocimiento teórico y práctico necesario para la implementación.

Por lo general las empresas intentan ahorrar dinero y no contratan algún tipo de asesoría para guiar el proyecto, finalmente no se consiguen los objetivos propuestos o resulta una solución mucho más costosa, en este caso aplica el conocido refrán "lo barato sale caro".

El exceso de confianza es otro de los elementos que evidencian una exigua experiencia, pensar que la implementación se puede hacer en unos pocos meses es subestimar la cantidad y la calidad del trabajo que se debe realizar, da como resultado una serie de documentos, políticas y procedimientos que nadie usará o peor aún que nadie siquiera la perciba.

Seguridad de la información más que documentos, políticas, riesgos, controles, procedimientos, etc., es generar una cultura organizacional, la "cultura de seguridad de la información" requiere tiempo. En el cambio cultural reside el éxito del sistema de gestión de seguridad de la información, pero como es un cambio, la resistencia es precisamente su principal obstáculo. Por ejemplo, al implementar una política de claves fuertes y cambio periódico, seguramente muchos empleados reaccionaran negativamente con la política o al desplegar el proceso de reporte de incidentes, muchos no lo notificaran, como estos hay un sin número de casos que afectan de manera critica el proceso, por consiguiente la calidad del programa de capacitación y concienciación juega un papel crítico para vencer esta resistencia. De forma paralela con la introducción de nuevas herramientas, es seguro que los empleados necesiten de nuevas habilidades que inicialmente deben adquirirse a través de capacitaciones, mientras se logra la experticia suficiente.

Dependiendo de los recursos financieros con que se cuente para el proyecto, la premura del tiempo y la calidad de la documentación, es necesario establecer la mejor opción de para abordar la implementación, ya sea si se encamina por una auto-implementación o por el contrario se contrata la totalidad a manos expertas o una combinación entre estas dos. A continuación se muestra los pros y contras de estas tres opciones.

1. *Auto-implementación - Implementar únicamente con los empleados*: En apariencia esta opción es la más económica, pero lleva más tiempo debido a que obligatoriamente tiene que averiguar cada paso, elaborar cada documento y capacitar, además de que conlleva un alto grado de incertidumbre sobre el resultado final del proyecto. Por la falta de experiencia se cometerán muchos errores y omisiones lo que finalmente se convierte en sobre costo, frecuentemente luego de varios meses e incluso de años, las organizaciones encuentran que han desperdiciado mucho tiempo y dinero, y sin ningún resultado.

Pero no todo es malo en esta alternativa, ya que al involucrar de lleno a quienes conocen los procesos de la empresa se obtiene un gran alcance en capacitación y concienciación. Por otra parte y de acuerdo con Dejan Kosutic en [5], esta opción "es la mejor si usted tiene cuestiones de alta confidencialidad, ya que no querrá dejar que nadie externo conozca por dentro a su empresa."

2. *Implementar utilizando principalmente manos expertas*: Como ya se dijo es importante tener en cuenta el costo y el tiempo del proyecto; precisamente esta alternativa ofrece mejor tiempo, sin embargo puede ser más costosa debido al precio de una asesoría de calidad, la documentación será de buena calidad, pero es seguro que se presente algún tipo de resistencia al desplegar políticas y procedimientos, la transferencia de conocimiento será algo escasa dado el costo de la misma y solo algunos empleados gozaran de este beneficio.

3. *Auto-implementación con asesoría experta*: En esta opción brinda adecuada proporción entre costo y tiempo, ya que gran parte de las actividades serán realizadas por los empleados bajo la guía y supervisión de asesor experto, optimizando así el costo por errores. Cuando la documentación es realizada por personal interno, se logra un mayor nivel de compromiso con las nuevas reglas y políticas, respecto a la trasferencia de conocimiento es posible obtener un adecuado balance con apropiados programas de capacitación.

E. **No se realiza seguimiento ni mantenimiento a la implementación.**

Luego del proceso de implementación del Sistema de Gestión de Seguridad de la Información (SGSI), sigue un proceso continuo de mantenimiento, que según la ISO 27001 en la sección 8 – Funcionamiento y sección 9 – Evaluación del desempeño, proponen una serie de actividades que deben ser realizadas permanentemente para lograr la efectividad del sistema.

Es lamentable que luego de todo el esfuerzo hecho para la implementación del SGSI, se dejen de lado las políticas, los procedimientos, los controles, el plan de riesgos, la tecnología, etc., porque son obsoletas, inservibles o nunca

fueron actualizadas, lo que demuestra un claro fracaso e inoperancia del sistema. Para que esto no suceda es importante tener en cuenta una serie de actividades propuestas desde la norma ISO 27001.

1. *Se debe medir*: "Lo que no se mide no se puede controlar", aquí no hay opción, si se quiere controlar algo tenemos que medirlo y finalmente se debe determinar si se están cumpliendo los objetivos, si los controles están siendo efectivos, si el costo está entre los parámetros planeados, etc. La medición debe permitir compararse con otros periodos y así determinar una tendencia.
2. *Se debe supervisar*: En este punto es importante la inspección de los controles planteados, verificar su efectividad, determinar errores o incidentes para evitar la recurrencia.
3. *Se debe auditar*: La ejecución de un programa de auditoria al SGSI, es muy importante y útil para determinar que las cosas se están realizando según lo planeado y no de manera contraria. Con el día a día es muy difícil determinar en qué se está fallando, la mirada objetiva y minuciosa de un auditor calificado determinará el cumplimiento o la no conformidad del sistema. Aquí se plantea u proceso de mejoramiento continuo, en donde las medidas preventivas y correctivas deben ser implementadas y evaluadas, además deben garantizar que el problema detectado fue realmente eliminado.
4. *La gerencia debe revisar el sistema:* No solamente para determinar si el ROSI es positivo, también debe verificar los resultados de la medición, de las auditorias, de los controles, de los niveles de riesgo, entre otros y así tomar las decisiones importantes sobre el curso del SGSI.

Luego de un recorrido por estos cuatro planteamientos, donde se revela la importancia de cada uno de ellos durante la implementación del SGSI, solo resta decir que un abordaje superficial, una mala interpretación o aplicación simplista de cualquiera de estas proposiciones, deja como resultado un proceso deteriorado, con graves desperdicios que generan altos costos y gastos a la organización.

III CONCLUSIONES

La Tecnología de la Información (TI) es muy importante en el contexto general de la seguridad de la información, siempre y cuando se considere como una herramienta para mitigar los riesgos y no como el único instrumento de seguridad.

Las implementaciones de SGSI que carecen de apoyo y orientación de la alta gerencia serán más difíciles y propensas a no alcanzar los objetivos propuestos. Sin este apoyo, seguramente el gestor del proyecto quedará como el responsable de un proyecto fallido.

Para que la alta dirección comprenda de qué se está hablando, se debe utilizar su mismo idioma y se debe entender su forma de pensar, que generalmente se reduce a "rendimiento de la inversión". Además, se tiene que llegar a ellos antes de comenzar con el proyecto, porque de lo contrario los problemas serán de mayor orden.

La seguridad de la Información debe ser vista como un proyecto integral de y para toda la empresa, que involucra empleados, unidades de negocio, la alta dirección, el personal de TI, expertos legales, líderes de procesos, personal administrativo y misional, etc. Sin este enfoque se acabará trabajando en la seguridad de TI, la cual aporta menos del 40% de los controles necesarios para la protección total de la organización.

Como la Seguridad de la Información es un proceso transversal a la organización, los programas de capacitación y concienciación deben platearse de la misma manera, estos deben ser planificados y con intensidad variable, dependiendo del público objeto y del grado de sensibilización requerido.

La falta de comunicación sobre el progreso del proyecto al personal de la organización, genera apatía a la comunidad en general, al contrario una comunicación efectiva los incentiva e involucra de manera proactiva. Del mismo modo la falta de acuerdos entre los interesados puede entorpecer el desarrollo del proyecto de implementación.

La implementación del SGSI no es algo que pueda ser realizado en poco tiempo y solo con la lectura de un marco referencial. Dependiendo de los recursos financieros, del tiempo y la calidad de la documentación, se debe establecer el planteamiento de la implementación: auto-implementación, implementación por expertos o una combinación entre estas dos.

REFERENCIAS

[1] J.M San Martin G, "La Seguridad de la Información Nueva ventaja competitiva en la empresa (I/IV)" [Online]. Disponible: http://dialnet.unirioja.es/servlet/articulo;jsessionid=14432189D775360F21145B837ECC2C47.dialnet01?codigo=824400

[2] Dejan Kosutic, (Nov 2014). "Information security or IT security?" [Online]. Disponible: www.iso27001standard.com/blog/2010/03/01/information-security-or-it-security

[3] Christian Locher, (Ene 2005). "Methodologies for evaluating information security investments" [Online]. Disponible: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1136&context=ecis2005

[4] Richard. (2012, Jul 27). Project Management - Gestión de Proyectos [Mensaje de Blog]. Recuperado de http://richard-project-management.blogspot.com/2012/07/definicion-de-proyecto-segun-el-pmbok.html

[5] Dejan Kosutic, (2012). "Ciberseguridad en 9 pasos", Ed. EPPS Services Ltd, 2012, pp. 55-57 [Online]. Disponible: http://www.iso27001standard.com/es/books/ciberseguridad-en-9-pasos-el-manual-sobre-seguridad-de-la-informacion-para-el-gerente/

[6] Norma Técnica NTC-ISO-IEC Colombiana 27001-2013, (2013, Dic 11). "Tecnología de la información: Técnicas de seguridad. Sistemas de gestión de seguridad de la información: Requisitos"