"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DE CONSULTORÍA Y AUDITORÍA, APLICANDO LA NORMA ISO/IEC 27001"

Diana Tola F. [(1)], Lenin Freire C. [(2)]
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
dtola@espol.edu.ec [(1)], lfreire@espol.edu.ec [(2)]

Resumen

En los últimos años, con el desarrollo de las tecnologías de información y su relación directa con los objetivos de las organizaciones, el universo de amenazas y vulnerabilidades crece, por lo tanto es necesario proteger uno de los activos más importantes de la organización, la información, garantizando siempre la disponibilidad, confidencialidad e integridad de la misma.

La forma más adecuada para proteger los activos de información, es mediante una correcta gestión del riesgo, para así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentran más expuestos.

El presente proyecto de titulación reúne la información necesaria para la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la norma IO 27001:2005, para asegurar la protección de los activos de información y otorgar confianza a los clientes de A&CGroup S.A. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

Palabras Claves: *SGSI, ESPOL, tecnologías, disponibilidad, confidencialidad, integridad, información, amenazas, vulnerabilidades, organizaciones, proteger, implementación, ISO, seguridad, activos, gestión, FIEC.*

Abstract

In the last years, with the development of information technologies and their direct relation to the objectives of the organizations, the universe of threats and vulnerabilities is growing, so is necessary to protect one of the most important assets of the organization, information, guaranteeing the availability, confidentiality and integrity of the same.

The most appropriate way to protect information assets is through proper risk management in order to identify and focus efforts on those elements that are most exposed.

This titling project gathers the necessary information for the implementation of a Management System Information Security, based on the ISO 27001:2005 to ensure the protection of information assets and give confidence to customers of A&CGroup S.A. The standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS.

Keywords*: ISMS, ESPOL, technologies, availability, confidentiality, integrity, information, threats, vulnerabilities, organizations, protect, implementation, ISO, security, assets, management, FIEC.*

1. Introducción

El desarrollo de la tecnología de información y su relación directa con los objetivos de las empresas, las amenazas y vulnerabilidades aumentan, por lo tanto es necesario proteger uno de los activos más importantes de la organización, la información, garantizando su disponibilidad, confidencialidad e integridad.

Debido a que existen diversos escenarios de amenazas, que en cualquier momento pueden presentarse, es necesario que el negocio cuente con una estrategia de continuidad claramente definida por cada escenario de amenaza identificado para poder reanudar las operaciones rápidamente.

La forma más adecuada para proteger los activos de información, es mediante una correcta gestión del riesgo, para así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentran más expuestos.

2. Marco Teórico

2.1 ISO

La Organización Internacional de Normalización, es una federación de alcance mundial integrada por cuerpos de estandarización nacionales de 157 países.

La ISO es una organización no gubernamental, cuya misión es promover el desarrollo de la estandarización y las actividades relacionadas, con el fin de facilitar el intercambio de servicios y bienes y promover la cooperación en la esfera de lo intelectual, científico, tecnológico y económico.

2.2 Estándar

Es una publicación que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional, con el objetivo de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología.

Los estándares ayudan a aumentar la fiabilidad y efectividad de materiales, productos, procesos o servicios que utilizan todas las partes interesadas (productos, vendedores, compradores, usuarios y reguladores).

2.3 ISO 27001

Es un estándar que proporciona un modelo para establecer, implementar, utilizar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Se basa en un ciclo de vida PDCA o ciclo de Deming, de mejora continua.

2.4 Seguridad de la Información

Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información, buscando mantener la confidencialidad, disponibilidad e integridad de la misma.

3. Antecedentes

3.1 Descripción del Problema

En los últimos años, el uso de las tecnologías de la información dentro de las organizaciones ha ido aumentando rápidamente, ya que nos ayudan a optimizar las actividades de cada proceso de negocio, convirtiéndose en una herramienta valiosa. Así mismo la continua evolución de la tecnología, indudablemente representa una fuente de posibles riesgos para las compañías, que pueden provocar graves afectaciones, ya sean de tipo financiero, operacional y de reputación en las empresas.

En la actualidad uno de los activos más importantes que poseen las organizaciones, es la información, sin embargo en muchas ocasiones éstas no cuentan con políticas adecuadas para protegerla, generando vulnerabilidades que pueden ser aprovechadas por las amenazas existentes en el entorno y dar como resultado riesgos. El comportamiento observado en las organizaciones ante esta situación mayormente es reactivo.

3.2 Solución Propuesta

La forma más adecuada para proteger los activos de información, es mediante una correcta gestión del riesgo, para identificar y focalizar esfuerzos hacia aquellos elementos que se encuentran más expuestos, sobre todo para las empresas dedicadas a la auditoría financiera, como es el caso de A&CGroup S.A., que maneja información sensible de cada uno de sus clientes y por tanto es de vital importancia tener protegida dicha información.

El presente proyecto reúne la información necesaria para la implementación de un Sistema de Gestión de la Seguridad de la Información, basado en la norma ISO 27001:2005, para así garantizar la protección de los activos de información y otorgar confianza a cualquiera de las partes interesadas, sobre todo a los clientes.

La correcta implementación de un SGSI, ayudará a prevenir incidentes de seguridad, que generan pérdidas económicas e interrupciones en la continuidad del negocio, mediante la reducción de las probabilidades o impactos que los riesgos identificados pudieran ocasionar a su información.

3.3 Objetivo General

Lograr la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001:2005 para preservar la confidencialidad, integridad y disponibilidad de la información que maneja la empresa A&CGroup S.A.

3.4 Objetivos Específicos

1. Definir el alcance, objetivos y políticas del SGSI.
2. Identificar los riesgos sobre los activos definidos en el alcance del SGSI.
3. Analizar las probabilidades e impactos de los riesgos sobre los activos identificados bajo el alcance y calcular los niveles de riesgo, aplicando la metodología MAGERIT.
4. Implementar controles sobre los activos, basado en un plan de tratamiento del riesgo.

5. Asegurar la creación de procedimientos para el monitoreo y revisión del sistema, que cubra: incidentes de seguridad, auditorías internas y revisiones gerenciales.

4. Levantamiento de Información

4.1 Antecedentes de la Empresa

A&CGroup S.A. es una empresa de servicios que opera en Ecuador con oficinas en Guayaquil y Quito. Sus principales actividades son la prestación de servicios de auditoría financiera externa y la consultoría empresarial en aspectos contables, tributarios y legales.

4.2 Identificación de procesos claves de la Empresa

El estándar ISO 27001 promueve la adopción de un enfoque de procesos para todas las fases del Sistema de Gestión de Seguridad de la Información. Así, los procesos que se vayan definiendo deben ser clasificados según su naturaleza dentro de una de las tres categorías siguientes: estratégicos, operativos y de soporte.

Dentro de A&CGroup S.A. tenemos como proceso estratégico a Gestión Gerencial Estratégica, como procesos operativos tenemos: Planeación, Realización y Finalización, como procesos de soporte tenemos: contabilidad, compras, auditoría interna, control de documentos, talento humano y gestión de seguridad.

En la figura 1 Mapa de procesos, se pueden observar los procesos estratégicos, operativos y de soporte de la empresa A&CGroup, junto con sus secuencias e interacciones de los mismos.

Figura 1. Mapa de procesos

4.3 Identificación de activos de información

El proceso de identificación de activos de información es muy importante, ya que nos permite reconocer cuales son los activos que se encuentran asociados a los procesos de la organización.

La realización de cada proceso involucra activos de información específicos, en sus diversos tipos y formatos, los cuales son listados en la tabla 1 Inventario de Activos que se muestra a continuación:

Tabla 1. Inventario de Activos

No.	Activo	Tipo de activo
1	Servidores	Hardware
2	Socio, Auditores	Persona
3	File Papeles de trabajo – documentos físicos	Datos/Soportes de información
4	Registros SGSI llenados (formato digital)	Datos/Soportes de información
5	Servicio de correo electrónico	Servicio
6	Red de área local e inalámbrica	Comunicaciones
7	Sistema META, SAFI	Software/ Información
8	Personal administrativo	Persona
9	Software ACL	Software/ Información
10	Sitio Web	Servicio
11	Sistema de comunicación telefónica IP	Comunicaciones
12	Computadores/Laptops	Hardware
13	Impresoras	Hardware

4.4 Diagnóstico de la situación actual de la empresa

Debido a la necesidad de implementar un SGSI, la empresa procede a realizar un diagnóstico de la situación actual respecto a los requisitos de la norma, con el fin de tener una idea de que mecanismos tiene instaurada la organización y que puedan aprovecharse para facilitar la implementación de los requisitos exigidos por ISO 27001.

5. Planeación para la implementación de un SGSI

5.1 Modelo PDCA (Plan – Do – Check – Act)

Este modelo es muy usado para la implantación de sistemas de gestión, en este caso un Sistema de Gestión de Seguridad de Información, ya que permite una efectiva organización y documentación.

En la figura 2 Modelo PDCA, se muestra este modelo basado en los procedimientos esenciales para un SGSI.

Figura 2. Modelo PDCA

5.2 Alcance

En la actualidad existen muchos aspectos que se deben tener en cuenta para asegurar que se cumplan con las expectativas requeridas. Por lo tanto, se debe disponer de todos los recursos para garantizar la seguridad de la información, como es el caso de A&CGroup, que maneja información sensible de sus clientes.

El alcance del SGSI cubrirá las operaciones contenidas en los procesos de Planeación, Realización y Finalización de servicios de auditoría financiera externa.

5.3 Objetivo General

Proporcionar a la alta gerencia las directrices y el soporte para la seguridad de la información, es decir qué requiere ser protegido, por qué, de qué debe ser protegido y cómo protegerlo; acorde con los requerimientos comerciales, leyes y regulaciones relevantes.

5.4 Políticas de Seguridad

Estas políticas representan directrices que deben ser adoptadas por el personal de la empresa:

1. Los usuarios solo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
2. Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
3. Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
4. El ingreso de las personas a la oficina será restringido con el uso de un mecanismo electrónico de control de accesos basado en lector de huellas dactilares.
5. El acceso al cuarto de servidores estará limitado al responsable del área de Tecnología y Sistemas de Información. Para el ingreso se contará con un mecanismo electrónico de control de accesos basado en lector de huellas dactilares.
6. Las contraseñas contendrán al menos 3 referencias de los siguientes caracteres: números, letras mayúsculas, letras minúsculas, símbolos y que tenga mínimo 8 caracteres de longitud.

6. Análisis de riesgo, diseño de la evaluación del riesgo

6.1 Metodología de control de riesgo

Debido a que las condiciones económicas, industriales, normativas y operacionales se modifican de forma continua, se hacen necesarios mecanismos para identificar y minimizar los riesgos específicos asociados con este cambio.

Por tal motivo, existen varias metodologías para realizar el análisis de riesgo, por tanto debemos seleccionar la más adecuada acorde a la realidad de la empresa.

6.2 Metodología MAGERIT

Es una metodología de análisis y gestión de riesgos que proporciona un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información, para así poder implementar las medidas de control más adecuadas que permitan mitigar los riesgos.

Esta metodología es muy útil, ya que permite enfocar los esfuerzos en los riesgos que puedan ser más críticos para la empresa, aquellos relacionados con los sistemas de información.

6.3 Ventajas de la Metodología

- Las decisiones que deban tomarse y que tengan que ser validadas por la dirección, estarán fundamentadas y serán fácilmente defendibles.
- Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla.
- Permitirá saber cuánto valor tiene la información o los servicios que maneja la empresa.
- Conocer el riesgo al que están sometidos los elementos de trabajo para poder gestionarlos.

- Tener una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

En la figura 3, se puede observar la metodología.

Figura 3. Metodología MAGERIT

6.4 Análisis del Riesgo

Contempla las siguientes fases:

1. Identificación de activos de información.
2. Identificación de requerimientos legales y comerciales que son relevantes para los activos identificados.
3. Tasación de los activos identificados.
4. Identificación de amenazas y vulnerabilidades para cada activo previamente identificado.
5. Cálculo de la posibilidad de que las amenazas y vulnerabilidades ocurran.

6.4.1. Inventario de Activos. En la organización, el proceso de identificación y tasación de activos debe realizarlo un grupo multidisciplinario compuesto por personas involucradas en los procesos y subprocesos que abarca el alcance del modelo. Es importante que los dueños de los activos principales conformen un grupo. Dentro del alcance del SGSI, los activos importantes deben identificarse con claridad y posteriormente deben ser tasados para visualizar su impacto en la empresa por su deterioro o por fallas en: confidencialidad, integridad y disponibilidad.

6.4.2. Identificación de requerimientos legales y comerciales. Los requerimientos de seguridad en las organizaciones se derivan de tres fuentes:

1. La evaluación de los riesgos que afectan a la organización.
2. El aspecto legal.
3. El conjunto de principios, objetivos y requerimientos para procesar información, que la empresa ha desarrollado para apoyar sus operaciones.

6.4.3. Tasación de Activos. El proceso de identificación y tasación de activos, tiene como objetivo conocer el valor que poseen los activos para la organización y así comprender cuales tienen una mayor relevancia. La forma de conocer el valor de un activo, es indagando que tanto impactaría en el negocio un deterioro o pérdida de confidencialidad, integridad o disponibilidad en el mencionado activo. Así podremos conocer que tan crítica y sensible es la información manejada en la organización. El valor de un activo vendrá definido por el promedio de la afectación a la integridad, disponibilidad y confidencialidad para su respectivo proceso.

6.4.4. Identificación de amenazas y vulnerabilidades. En las organizaciones, los activos de información están sujetos a distintas formas de amenazas, que pueden causar un incidente no deseado que puede generar daño a la organización y a sus activos. Cuando la empresa inicia la identificación de amenazas que pudiesen afectar sus activos, conviene clasificarlas por su naturaleza. Una amenaza puede originarse de fuentes o eventos accidentales y para que cause daño a algún activo, tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por la organización. Una vez identificadas las amenazas, también es importante proceder a identificar las vulnerabilidades existentes en los activos de información, ya que son condiciones que pueden hacer que una amenaza afecte un activo.

6.4.5. Cálculo de probabilidad de que las amenazas y vulnerabilidades ocurran. Una vez identificadas las amenazas y vulnerabilidades, es necesario calcular la posibilidad de que puedan juntarse y causar un riesgo. El objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos y en el cálculo de las amenazas y vulnerabilidades.

6.5 Evaluación del Riesgo

Para realizar la evaluación del riesgo, se recomienda crear una escala para medir los niveles de riesgo. Los criterios que usualmente se recomiendan para esto son:

- Impacto económico del riesgo.
- Tiempo de recuperación de la empresa.
- Posibilidad real de ocurrencia del riesgo.
- Posibilidad de interrumpir las actividades de la empresa.

Una vez identificados los criterios, se debe elaborar una escala para realizar la evaluación y determinar los grados de importancia que representan las amenazas para la empresa.

6.5.1. Cálculo del Riesgo. Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas de confidencialidad,

integridad y disponibilidad y del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente. Estos valores nos van a proveer un medio para poder priorizar los riesgos e identificar aquellos otros riesgos que son más problemáticos para la organización.
El método para el cálculo del riesgo trata de relacionar los factores del impacto económico de la amenaza y la probabilidad de ocurrencia de la amenaza.
Posteriormente se debe calcular la medición del riesgo, multiplicando los valores obtenidos del impacto de la amenaza y la probabilidad de ocurrencia de dicha amenaza. Finalmente las amenazas pueden ordenarse, de acuerdo a su factor de exposición al riesgo.

6.5.2. Estrategias para el tratamiento del riesgo.
Después de realizar el análisis y la evaluación del riesgo, se debe pensar en qué acciones se van a tomar con esos activos que están sujetos a riesgos.
Existen 4 estrategias para el tratamiento del riesgo, que son:

1. Reducir.
2. Evitar
3. Transferir
4. Aceptar

7. Implementación de un sistema de gestión de seguridad de la información

7.1 Plan de Tratamiento del Riesgo

Una vez que se realiza el proceso de identificar las opciones de tratamiento del riesgo y haberlas evaluado, la empresa debe decidir cuales objetivos de control y controles debe escoger para el tratamiento.

La selección de estos controles, se debe hacer tomando en cuenta el criterio establecido para la aceptación del riesgo y los requerimientos legales y contractuales.

Es importante saber que los objetivos de control y controles se deben seleccionar del Anexo A de la norma ISO 27001.

Después de implementar las decisiones relacionadas con el tratamiento del riesgo, siempre habrá un residuo de ese mismo riesgo, al cual se lo denomina “Riesgo residual”.

Otro documento que interviene en esta fase, es la declaración de aplicabilidad, cuyo objetivo es incluir todos los objetivos de control y controles escogidos del Anexo A que son relevantes para el SGSI y aplicables a la organización. También se debe detallar la exclusión de cualquier objetivo de control y control, con su respectiva explicación.

7.2 Políticas

7.2.1. Políticas Generales.

- Los usuarios solo deben tener acceso a los servicios para los cuales han sido autorizados.
- Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
- Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
- En caso de que necesite alejarse del computador, debe bloquear la sesión activa.
- Los archivos creados deberán ser almacenados en el repositorio establecido por la empresa.

7.2.2. Políticas de seguridad a nivel físico.

- El ingreso de las personas a la oficina será restringido con el uso de un mecanismo electrónico de control de accesos basado en lector de huellas dactilares.
- Todo el personal debe contar con su respectiva tarjeta de identificación.
- El personal externo deberá recibir una tarjeta de visita.
- El ingreso y salida de Files del cuarto de archivo deberá ser registrado en una bitácora por una persona del departamento de administración.

7.2.3. Políticas de seguridad a nivel lógico.

- Todo equipo con sistema operativo Windows tiene activo el firewall de comunicaciones para evitar infección y posibles ataques al computador.
- Todos los equipos de Windows cuentan con software antivirus.
- Todo archivo de dudosa procedencia se debe rechazar.
- No conectarse a redes inalámbricas inseguras si se va a trabajar con información confidencial de la empresa.

7.2.4. Políticas de respaldo y recuperación de información.

- Las copias de respaldo de la información se realizarán dos veces en el día a intervalos definidos.
- Los respaldos se harán mediante la herramienta correspondiente y serán almacenados en una unidad de almacenamiento externo.
- Se deben realizar pruebas de restauración, al menos una vez al año.

7.2.5. Políticas de mantenimiento de equipos.

- Antes de encender el computador asegúrese que se cuente con condiciones ambientales adecuadas.
- Al finalizar la jornada laboral se debe apagar el sistema haciendo uso de la opción apagar.
- Cuando el laptop se encuentre cerrado evitar colocar carpetas o elementos encima del mismo.
- No consumir bebidas en los escritorios de trabajo donde se encuentren equipos de computación y/o documentos físicos.

7.2.6. Políticas de uso de software.

- Los usuarios no deben instalar o intentar instalar programas, utilitarios o complementos para navegadores de internet.
- Está prohibido el uso de programas sin licencias no autorizadas por la empresa.
- Todo equipo de computación debe mantener en forma residente un antivirus instalado y las actualizaciones deben realizarse en línea.

8. Análisis de Resultados

8.1 Estrategias de difusión

La última fase de un Sistema de Gestión de Seguridad de la Información consiste en la concientización y formación del personal, con el fin de crear una cultura de seguridad dentro de la organización.

Las estrategias utilizadas por A&CGroup para lograr esto son:

- Programa de capacitación en seguridad de la información.
- Campaña de concientización.

8.1.1. Programa de capacitación en seguridad de la información. Consiste en un grupo de videos, debajo de cada uno se encuentra una sección que contiene el acceso a una autoevaluación en línea referente al video visto previamente, tal como se muestra en la figura 4.

Figura 4. Programa de capacitación

8.1.2. Campaña de concientización para el personal. Otra estrategia de concientización utilizada es la campaña de concientización para el personal, la cual consiste en un grupo de fondos y protectores de pantalla, los cuales contienen las políticas más relevantes para lograr mantener la seguridad de la información, tal como se muestra en la figura 5.

Figura 5. Campaña de concientización

8.2 Reporte de incidentes de seguridad de la información

Tiene como finalidad asegurar que la información de los eventos y debilidades en la seguridad de la información, sea comunicada para así poder tomar una acción correctiva oportuna.

El objetivo de esta actividad es proveer un canal de comunicación para que el personal pueda dar a conocer los eventos o incidentes y asegurar el tratamiento de los mismos. En la figura 6, se observa la pantalla del sistema utilizado para realizar el reporte de los incidentes.

Figura 6. Reporte de incidentes de seguridad de la información.

9. Conclusiones

1. Debido a que en las organizaciones es primordial la optimización de recursos, el establecimiento del alcance del sistema de gestión de seguridad de la información se convierte en una actividad muy importante ya que delimita el campo de acción y el uso de recursos.
2. Es importante establecer los objetivos y políticas del sistema de gestión de seguridad de la información, ya que estos van delineando el camino hacia donde la organización desea dirigirse para preservar la confidencialidad, integridad y disponibilidad de la información y por lo tanto es relevante la participación de la alta gerencia.
3. La adopción de la metodología MAGERIT para el análisis de riesgos, permitirá identificar de manera oportuna la probabilidad y el impacto de que se materialicen los riesgos y de esta manera poder establecer controles que nos ayuden a prevenirlos.
4. Los sistemas de Gestión de Seguridad de Información bajo la norma ISO 27001, se basan en la prevención, por lo tanto es muy importante identificar los riesgos a los que están expuestos los activos para así evitar pérdidas económicas u operacionales.
5. Una vez identificados los riesgos a los que están expuestos los activos de información, es necesario implementar controles o salvaguardas, con la finalidad de proteger estos activos y lograr minimizar la probabilidad de que se materialicen los riesgos o el impacto que pueden tener sobre la organización. Es importante considerar que al momento de seleccionar los controles se debe realizar un análisis de costo beneficio ya que el costo de la implementación de un control no debe exceder la posible pérdida económica de no tener implementado el control.
6. Dentro del ciclo de un Sistema de Gestión de Seguridad de la Información, basado en ISO 27001, se encuentra la mejora continua lo cual hace que sea muy importante que la organización se asegure de crear procedimientos para el monitoreo y revisión del sistema, los mismos que deben cubrir incidentes de seguridad, auditorías internas y revisiones gerenciales. Estos elementos aportan retroalimentación al Sistema posibilitando conocer el estado del mismo y aplicar acciones correctivas, si fuera el caso, que permitan el cumplimiento de los planes y objetivos

10. Recomendaciones

1. La concientización de la compañía es un pilar fundamental de esta norma, por lo cual la organización debe poner mucho empeño en despertar el interés y compromiso de todos sus empleados.
2. Contar con personal clave dentro de la empresa y con las competencias exigidas por la Norma ISO 27001:2005 para evitar la contratación de consultorías externas, cuyo costo suele ser alto.
3. La organización debe tratar de facilitar las tareas operativas del sistema SGSI, para lo cual necesita utilizar herramientas tecnológicas que automaticen ciertas tareas.
4. Se debe buscar el compromiso y soporte gerencial, de manera que el proyecto venga patrocinado desde arriba en la dirección, y sea esta la primera en dar ejemplo a la hora de aplicar aquellas medidas necesarias para definir, aplicar y mantener la seguridad en la empresa.
5. Es importante que se establezca un sistema de medición, que permita valorar la marcha del SGSI de modo global y particular, detectando desviaciones y cambios en la empresa que deban ser tratados para que el SGSI se mantenga operativo.

11. Referencias

[1] Organización Internacional para la Estandarización (ISO).

http://www.bajacalifornia.gob.mx/registrocivilbc/iso_informa2.htm
[2] Norma ISO27001.
http://www.iso27000.es/iso27000.html
[3] Alberto G. Alexander. Diseño de un Sistema de Gestión de Seguridad de Información- Óptica ISO 27001:2005. Alfaomega, 2007
[4] Ministerio de Hacienda y Administraciones Públicas – Gobierno de España. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.