Implementación del Primer Sistema de Gestión de Seguridad de la Información, en el Ecuador, Certificado bajo la Norma ISO27001:2005

José Alfonso Aranda Segovia
Facultad de Ingeniería en Electricidad y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil, Ecuador
aaranda@telconet.net
Ing. Freddy Pincay
fpincay@espol.edu.ec

Resumen

Dada la evolución de la Tecnologías de la información y su relación directa con los objetivos del negocio de la organizaciones, el universo de amenazas y vulnerabilidades aumenta, por lo tanto es necesario proteger uno de los activos más importantes de la organización, la información, garantizando siempre la disponibilidad, la confidencialidad e integridad de la misma. La forma más adecuada para proteger los activos de información es mediante una correcta gestión del riesgo, logrando así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentren más expuestos.

La implementación de un Sistema de Gestión de Seguridad de la información garantiza que la organización adopte las buenas prácticas sugeridas por la ISO 27001:2005 para un correcto tratamiento del riesgo. A continuación, se expone un caso de éxito de una implementación de un SGSI y su respectiva certificación bajo la norma ISO 27001:2005

Palabras Claves: ISO27001:2005

Abstract

Given the evolution of information technologies and their direct relationship with the business objectives of organizations, the universe of threats and vulnerabilities increase, then is necessary to protect one of the most important assets of the organization, The information, ensuring always the availability, confidentiality and integrity of it. The most appropriate way to protect information assets is through proper risk management, achieving identify and focus efforts on those elements that are most exposed.

Implementing a Information Security Management System guarantees to organization that adopt the best practices recommended by the ISO 27001:2005 for the proper treatment of risk. Then we are going to show a successful case in the implementation of an ISMS and their respective certification under the ISO 27001:2005

1. Introducción

En la actualidad uno de los principales activos que las organizaciones poseen, es la información. Por lo cual es necesario que toda organización que busque una excelencia en los servicios o productos que ofrece, adopte una Sistema de Gestión para el manejo adecuado de la información, garantizando así su disponibilidad, confidencialidad e integridad. Toda organización que desee convertirse en un proveedor confiable debería garantizar la continuidad de su negocio ante posibles escenarios de amenazas que pudieran presentarse.

Para cubrir estas necesidades la ISO - Organización Internacional para la Estandarización- creó una norma certificable que permite a las organizaciones encaminarse en un Sistema de Gestión de Seguridad de la Información, la ISO 27001:2005.

1.1. ¿Qué es un Sistema de Gestión de Mejora Continua?

Según el British Standard Institute es una estructura probada para la gestión y mejora continua de las políticas, los procedimientos y procesos de la organización. Las empresas que operan en el siglo XXI se enfrentan a muchos retos, significativos, entre ellos: Rentabilidad, competitividad, globalización, velocidad de los cambios, capacidad de adaptación, crecimiento y tecnología. Equilibrar estos y otros requisitos empresariales puede constituir un proceso difícil y desalentador. Es aquí donde entran en juego los sistemas de gestión, al permitir aprovechar y desarrollar el potencial existente en la organización.

La implementación de un sistema de gestión eficaz puede ayudar a:

- Gestionar los riesgos sociales, medioambientales y financieros.
- Mejorar la efectividad operativa.
- Reducir costos.
- Aumentar la satisfacción de clientes y partes interesadas.
- Proteger la marca y la reputación.
- Lograr mejoras continuas.
- Potenciar la innovación.
- Eliminar las barreras al comercio.
- Aportar claridad al mercado.

El uso de un sistema de gestión probado le permite renovar constantemente su objetivo, sus estrategias, sus operaciones y niveles de servicio.

1.2. ¿Qué es la Norma ISO 27001:2005?.

Es la normativa certificable para los Sistemas de Gestión de Seguridad de la Información, la cual evolucionó del estándar ISO 17799 que a su vez se derivó de la BS 7799. La finalidad de esta norma es permitir de forma sistemática minimizar el riesgo y proteger la información en las empresas.

La norma ISO 27701:2005 está constituida por 8 clausulas y Anexos, de los cuales la parte medular del sistema son desde la cláusula 4 a la 8 y el Anexo A. Las cláusulas indican los procedimientos que deben ser implementados, los documentos que deben ser elaborados y los registros que deben ser mantenidos dentro de la organización. El anexo A indica los controles y objetivos de control a implementar con el fin de ser salvaguardas o contramedidas, los mismos que se encuentran distribuidos en 11 dominios de cobertura que son:

- A.5. Política de seguridad
- A.6. Organización de la seguridad de la información.
- A.7. Gestión de activos.
- A.8. Seguridad de los recursos humanos.
- A.9. Seguridad física y ambiental.
- A.10. Gestión de las comunicaciones y operaciones.
- A.11. Control de acceso.
- A.12. Adquisición, desarrollo y mantenimiento de los sistemas de información.
- A.13. Gestión de incidentes en seguridad de la información.
- A.14. Gestión de la continuidad del negocio
- A.15. Cumplimiento.

La metodología de los sistemas de gestión se basa en el Ciclo de Deming, llamado así en honor a su creador el estadista estadounidense William Edwards Deming, cuyas pasos son: Planear, Implantar, Revisar y Mejorar o PLAN-DO-CHECK-ACT (PDCA). La representación gráfica del ciclo de Deming abstrae el concepto de mejora continua por la retroalimentación del paso final al paso inicial.

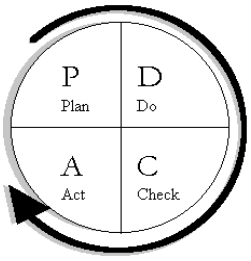

Figura 1. Ciclo de Deming.

Las clausulas de la Norma se distribuyen usando como base el ciclo en mención cuya adopción operativa en la organización, constituye un factor

clave para el Sistema de Gestión de Seguridad de la información (SGSI) o Information Security Management System (ISMS) por sus siglas en inglés .

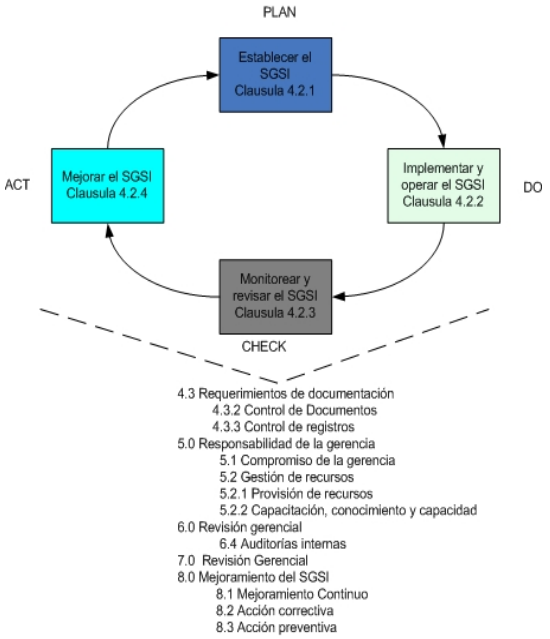

Figura 2. Clausulas de la Norma ISO 27001 distribuidas en Ciclo de Deming.

2. Metodología de implantación.

La metodología de implantación debe desarrollarse acorde a la cláusulas 4.2 descrita en la Norma ISO 27001:2005 correspondiente al establecimiento y operación de SGSI. La misma que nos indica que debemos definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance.

La definición del alcance del sistema es responsabilidad de la dirección de la organización bajo el asesoramiento del equipo de trabajo destinado a la gerencia del proyecto. También se acostumbra , para la toma de decisiones coyunturales, constituir un comité de seguridad liderado por el Director o Gerente General y conformado por Gerencias de diferentes áreas como la de tecnología, financiera, Recursos Humanos, Comercial, operaciones, etc.

El alcance para el proveedor de Servicio de Telecomunicaciones es:

"La provisión de un sistema de gestión de seguridad de información, para los procesos de: monitoreo, control de cambios, aprovisionamiento y mantenimiento de la red de telecomunicaciones en Guayaquil y Quito".

La clausula 4.2.1 de la norma también nos indica que debemos establecer una política de seguridad de la información acorde a las características del negocio, organización, activos, regulaciones y tecnología. Es muy poco exacto redactar una política de seguridad para toda la organización al iniciar el proceso de implantación, la buena práctica es redactarla en paralelo al proceso de acuerdo a las necesidades del sistema, que irán apareciendo. Lo que se recomienda es redactar una Política de Seguridad de Información GENERAL que guíe lo que queremos conseguir mediante nuestro SGSI. Para nuestro caso la política general es:

"Proveer Servicios de Telecomunicaciones con un Sistema de Gestión de Seguridad de la Información basado en la Prevención y enfocado a minimizar el riesgo de incidentes que atenten contra la confidencialidad, integridad y disponibilidad de la Red " .

2.1. Identificación los procesos.

La identificación de procesos dentro del alcance constituye un pilar fundamental para el enfoque del SGSI. En nuestro caso los procesos involucrados son: Monitoreo, Control de cambios, mantenimiento y aprovisionamiento.

Para una organización donde no exista una cultura de procesos o simplemente no se los tiene identificado es recomendable primero realizar un correcto levantamiento de procesos antes de avanzar con la implantación del SGSI.

2.1.1 Métodos de las elipses. El método de las elipses es un mecanismo que permite identificar dentro de un proceso todas las relaciones de sus subprocesos y actividades con otras áreas de la organización, y entidades externas. Una vez establecidas las relaciones es casi natural poder identificar los activos de información que se usan en dicha relaciones.

2.2. Identificación y tasación de activos.

Los activos de información pueden ser el software, el hardware, los enlaces, el equipamiento, los documentos, las personas que manejen (Procesen, trasladen, almacenen) información de valor para el negocio de la organización. El proceso de tasación de activo también es recomendado hacerlo mediante un taller multidisciplinario.

Las relaciones encontradas mediante el método de las elipses nos permitieron visualizar con claridad los activos involucrados. El siguiente paso es tasar el listado de los activos para quedarnos con aquellos de mayor valor. La pregunta para evaluar es ¿la pérdida

o deterioro de este activo, cómo afecta la disponibilidad, confidencialidad e integridad del proceso del negocio de la compañía? , en nuestro caso se usó la escala de 1 a 5, siendo el 1 de menor afectación y 5 de mayor afectación. El valor total del activo es el promedio entero de los valores asignados a la disponibilidad, confidencialidad e integridad. Una vez calculado el valor por cada activo, seleccionamos aquellos de mayor valor. El valor umbral queda a discreción de cada organización por ejemplo serán de importancia aquellos con un valor mayor a 3.

2.3. Metodologías del análisis y evaluación del riesgo.

De igual manera que en los pasos previos, el análisis y evaluación del riesgo se lo lleva a cabo en un taller multidisciplinario de la organización. Para el análisis y evaluación del riesgo, nos podemos acoger a cualquier metodología conocida, pero la exigencia de la norma es que dicha metodología arroje resultados comparables y reproducibles, esto quiere decir que el producto debe ser similar si la evaluación la hace otro grupo taller multidisciplinario o si lo hace el grupo taller inicial en otro momento.

La recomendación es usar un método cualitativo para el cálculo del riesgo, puesto que puede abarcar todos los activos con mayor facilidad. El método cuantitativo exigiría que todo sea llevado a valor monetario y en la mayoría de los casos esta tarea es complicada y/o tarda demasiado, puesto que no sólo implica el valor comercial de los activos sino también de la afectación que pueden tener su entorno.

Nuestra metodología consiste que para cada activo debemos identificar todas las amenazas existentes, la posibilidad de ocurrencia de estas amenazas, las vulnerabilidades que pueden hacer que dicha amenaza se materialice y la posibilidad que dicha amenaza penetre tal vulnerabilidad. El valor del riesgo está dado por el producto matemático del valor del activo, encontrado en la tasación, por el valor de la mayor de posibilidad de amenaza.

La escala para calcular las posibilidades es de 1 al 5, siendo 5 mayor. De la misma forma como en la tasación de activos se puede descartar las de menor valor para enfocarnos en las verdaderamente importantes, el valor del umbral es decisión del grupo taller.

La metodología expuesta puede irse sofisticando al ponderar los criterios de significancia del riesgo , por ejemplo cuanto afecta la imagen, el flujo de caja, ambiente laboral, pérdida de clientes, aspectos legales, satisfacción del cliente , participación del mercado , etc.

2.4. Tratamiento del riesgo.

El análisis y evaluación riesgo nos permitió valorizar el riesgo y conocer cuáles son los activos de información que tienen mayor exposición por lo tanto saber a dónde enfocar los recursos de la organización.

El riesgo tiene 4 opciones de tratamiento que son:

- Reducir el riesgo, con la aplicación de contramedidas o salvaguardas especificadas controles del Anexo A de la norma.
- Evitar el riesgo, dejando de realizar la actividad que produce el riesgo.
- Transferir el riesgo, a un tercero como por ejemplo una aseguradora o una tercerización de servicios.
- Aceptar el riego, que consiste en asumir la responsabilidad de correr dicho riesgo.

La opción de aceptación de un riesgo deber ser aprobada formalmente por la dirección de la compañía, en la mayoría de casos se presenta esta situación cuando el control necesario de implantar tiene un valor económico mayor que el mismo activo.

En nuestro caso la única opción de tratamiento que se usó fue la de reducción del riesgo.

2.4. Selección de controles.

Los controles son las contramedidas o salvaguardas especificadas en el Anexo A de la Norma ISO 27001:2005, enfocados a los 11 dominios de cobertura de la norma.

La selección de los controles que la organización debe implementar se lo hace por 3 fuentes:

- Del tratamiento del riesgo, orientados a eliminar vulnerabilidades o minimizar el impactos.
- Los requerimientos legales (implementación no es discutible).
- Producto de las operaciones en el negocio de la compañía.

Si se requiere una mayor ampliación de las prácticas para implementar los controles se puede referenciar a la ISO 17799:2005. También existe la posibilidad de que la organización cree sus propios controles puesto que los que se describen en la norma no se adapta a nuestras necesidades.

Uno de los requerimientos de la norma ISO 27001:2005 es que la organización cuente con una *DECLARACION DE LA APLICABILIDAD*, que consiste en un documento que comprometa e identifique los controles del anexo A de la Norma que se implementarán y la justificación en caso de que no proceda. Esto significa que por defecto todos los controles de la norma son aplicables a la organización y cualquier excepción debe ser justificada.

La declaración de aplicabilidad debe ser aprobada y revisada por la alta dirección de la empresa .

2.5. Medición de efectividad de los controles.

Una vez que los controles han sido implantados es necesario revisarlos constantemente que estén cumpliendo su objetivo. La medición de los controles se lo puede hacer mediante indicadores de efectividad, por ejemplo, si luego del análisis y evaluación de riesgo sobre el activo "Nodos Edge", salta a la luz que debemos implementar u optimizar el control A.9.2.2 de la Norma ISO 27001:2005 (Anexo A) cuyo objetivo de control son los servicios públicos y nos indica que los equipos deben ser protegido de fallas de energía y otras interrupciones por fallas de los servicios públicos. Los indicadores pueden ser de tipo seguimiento o de rendimiento, un indicador de seguimiento aplicado al control A.9.2.2 es el porcentaje de "Nodos Edges" por cada ciudad que pierde conectividad durante un apagón nacional.

Un indicador de rendimiento o performance puede ser el Tiempo de Supervivencia Real de un Nodo Edge durante un apagón / sobre el Tiempo Estimado de respaldo, este indicador nos mostraría que tan acertados han sido los trabajos de mantenimiento.

El indicador más significativo para un proveedor de servicio de telecomunicaciones es el llamado Acuerdo de Nivel de Servicios o SLA (Service Level Agreement) por sus siglas en inglés, establecido en los contratos, medido en porcentaje de disponibilidad del servicio. En términos generales consiste en calcular el tiempo de disponibilidad de un enlace dividido sobre el tiempo transcurrido. En implementaciones más sofisticadas el SLA también se puede ver afectado por variables o sub-indicadores como son el porcentaje de paquetes perdidos, jitter y/o delays.

Cada organización debe escoger los indicadores que económica y operativamente sean factibles implementar y llevar a cabo su medición. Pero sobre todas las cosas estas mediciones deben agregar valor a los objetivos del negocio de la compañía.

Algunos indicadores de tecnología son: porcentaje de falsos positivos de un IDS/IPS, porcentaje de disponibilidad de un Servidor WEB, porcentaje de solución de Incidentes que se extiende más de un tiempo X, Número de casos de Phishing presentados en el mes por ciudad, Número de Clientes que caen en listas negras de SPAM por Ciudad, Número de empleados infectados con virus por mes por ciudad.

La recomendación es que la medición de los indicadores debe institucionalizarse dentro de las operaciones del SGSI y conforme se optimice el sistema, dichas mediciones deben automatizarse.

2.6. Riesgos residuales.

El riesgo residual como su nombre lo indica, son aquellos riesgos remanentes aún cuando se haya implementado todos los controles necesarios. Los riesgos residuales deben ser conocidos, revisados y aprobados por la dirección de organización.

Conforme se optimiza el sistema estos riesgos residuales tienden a disminuir. Los riesgos residuales por lo general siempre están presentes puesto que llegar a riesgo cero es casi imposible ya sea porque el costo de un mayor control es muy alto o porque su posibilidad de ocurrencia es muy remota pero no cero. Por ejemplo , A pesar de implementar el control A.8.1.2 que nos indica que debemos contar con un proceso formal de selección de personal que incluyan test sicológicos, la verificación de antecedentes , siempre puede existir la posibilidad que un empleado descontento sabotee algún sistema.

Otros riesgos residuales comunes son: bugs de hardware o software desconocidos incluso por el fabricante, ataques que aprovechen vulnerabilidades de día cero, amenazas ambientales como tormentas eléctricas, derrumbes , que un empleado aún capacitado y evaluado contra ataques de ingeniería social sea vulnerado, etc.

2.7. Requisitos documentales.

En toda implementación de sistemas de gestión, un factor a superar es el sistema documental exigido por la norma, entre los principales motivos podemos mencionar:

- Se percibe como una carga operativa que no se quiere asumir.
- Rechazo al cambio.
- Informalidad muy institucionalizada.

Para poder obtener una certificación, hay que superarlo y utilizar mecanismos tecnológicos que faciliten la institucionalización del sistema

documental. La recomendación es implementar un sistema intranet que pudiera usar protocolo HTTPs y/o FTPS para la gestión de documentos. Dicho sistema debe manejar perfiles y roles así como también características del modelo AAA (Authentication, Authorization, Accounting).

La ISO 27001 tiene exigencias documentales que se indican en la cláusula 4.3 de dicha norma y son:

- Enunciado de la política de seguridad y los objetivos.
- El alcance del SGSI.
- Procedimientos y controles de soporte del SGSI.
- Una descripción de la metodología de evaluación del riesgo.
- Reporte de la evaluación del riesgo.
- Plan de tratamiento del riesgo.
- Enunciado o declaración de aplicabilidad.
- Procedimientos documentados necesarios por la organización para asegurar la planeación, operación y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles.
- Registros requeridos por este estándar internacional.

Los procedimientos documentados son:

- Debe existir un procedimiento documentados que especifique el manejo de documentos como es la creación, nomenclatura, aprobación, obsolescencia, cambios, etc.
- Debe existir un procedimiento documentado para el manejo de las auditorías, reporte de resultados y mantenimiento de registros.
- Debe existir un procedimiento documentado para el manejo de acciones correctivas.
- Debe existir un procedimiento documentado para el manejo de acciones preventivas.

Se deben mantener registros de:

- Auditorías realizadas.
- Resultados de las revisiones por la gerencia.
- Registros de capacitación, competencias, capacidades, experiencias y calificaciones.
- Y todos aquellos registros que otorguen evidencia objetiva del cumplimiento con la norma.

Una buena práctica es identificar textualmente todos los “debes” dentro de la redacción de la norma para así poder identificar las exigencias explícitas.

2.8 Factores de éxito

Existen factores que son claves para una implantación exitosa del sistema de gestión de seguridad de la información. Entre ellos podemos mencionar:

- Compromiso de la dirección con el SGSI.
- Objetivos del SGSI deben estar alineados con el negocio de la compañía.
- Liderazgo de la gerencia del proyecto.
- Motivación del personal.
- Concientización de toda la organización para con la seguridad.
- Embeber en todos los procesos del negocio el ciclo PLAN-DO-CHECK-ACT e institucionalizar la mejora continua.
- Establecer claramente las responsabilidades y obligaciones de cada persona dentro del SGSI.

3. Mejoramiento Continuo del SGSI.

Cuando una organización decide implementar un SGSI y certificarlo significa que ha tomado la decisión de encaminar sus operaciones en base a las mejores prácticas recomendadas por la Norma ISO27001:2005. Pero el verdadero éxito está en la sofisticación del sistema para ellos es necesario el mejoramiento continuo. El mejoramiento continuo está intrínseco en el modelo PLAN-DO-CHECK-ACT o Ciclo de Deming sobre el cual se basa los sistemas de gestión.

3.1 Mantenimiento y revisión del Sistema de Gestión de Seguridad de la Información.

La norma nos exige que el SGSI debe ser monitoreado y revisado, lo mismo que viene dado por los siguientes puntos:

- Medir la efectividad de los controles.
- Realizar auditorías interna.
- Realizar auditorías externas.
- Revisión por la dirección de todo el SGSI (cumplimiento de objetivos y resultados).
- Reuniones gerenciales para revisar acciones correcticas, acciones preventivas, oportunidades de mejoras.
- Correcta ejecución del procedimiento para reportar y tratar incidentes.
- Reevaluación de los riesgos cuando las condiciones de negocio o entorno cambien.
- Revisar los riesgos residuales.
- Sofisticación de los mecanismos de medición.

3.2. Metodología.

La metodología que la organización escoja para el mejoramiento continuo es flexible a la realidad tecnológica, operativa y económica de la organización. Pueden considerarse métricas de mejoramiento como son : número de proyectos de mejoras implantadas por un área en particular, la efectividad de una acción correctiva o preventiva, la disminución de tal o cual incidente, el ajuste de los controles a través del tiempo, la reducción de los riesgos residuales. La premisa de la metodología debe ser que no es necesario esperar una auditoría para emprender acciones correctivas, preventivas o proyectos de mejora.

Es importante tener claro el procedimiento de mejora continua, para saber cuándo abrir o cerrar una acción correctiva, preventiva u oportunidad de mejora.

Una acción correctiva (AC), se levanta ante algún incidente presentado o cuando alguna no conformidad con la norma haya sido detectada. Esta acción es cerrada únicamente cuando se puede comprobar la efectividad de la misma es decir cuando el incidente no vuelva a ocurrir.

Una acción preventiva (AP), se levanta para garantizar que un evento presentado no se convierta en un incidente.

Una oportunidad de mejora, como su nombre lo indique son aquellas actividades que se realizan sin necesidad de la presencia de un incidente o un evento, por lo general contribuyen directamente a la sofisticación del SGSI.

También se puede usar una acción curativa o inmediata, que consiste en aquella que permite cubrir el incidente hasta poder encaminar una acción correctiva. Para nuestro caso real, del proveedor de servicio de telecomunicaciones, el objetivo fue concientizar a la gente respecto al mejoramiento continuo e institucionalizar el correcto uso del formato y/o procedimiento. En una compañía como la nuestra las reuniones de planificación gerencial son continuas por lo cual nos enfocamos en adoptar formatos y medios tecnológicos de mejora continua en dichas reuniones y así no duplicar procedimientos ni documentación. Por ejemplo para cualquier actividad a realizarse durante la semana debe especificarse cual es su origen es decir debemos indicar si es una acción correctiva, acción preventiva u oportunidad de mejora. Cabe recalcar que el registro, operación y el cierre de dicha actividad ya estaban manejados por nuestros procedimientos operacionales

3.3. Factores de éxito.

Un factor clave para el establecimiento del mejoramiento continuo es que existan políticas claras establecidas y un impulso jerárquico desde la dirección. Entre los factores importantes podemos mencionar:

- Gerencias de área debe asumir tareas de seguimiento.
- Adaptar procesos actuales al ciclo PDCA.
- Tratar las tareas o proyectos como acciones correctivas, preventivas u oportunidades de mejora.
- Proveer herramientas tecnológicas que disminuyen gasto operativo.
- Establecer formatos adecuados y que estén adaptados a los objetivos del negocio (cosas que agreguen valor).
- Revisión del sistema de gestión o parte de él cuando un cambio del entorno del negocio se produzca.
- Establecer indicadores de rendimiento, revisarlos y actualizarlos. Es buena práctica revisar dichos indicadores cada mes.
- Todas las tareas de revisión y mejoras del SGSI deben ser reconocidas como aumento de responsabilidades y estar descritas en las funciones de cada empleado, por el departamento de recursos humanos.
- Establecer métricas de evaluación del personal basadas en el aporte al SGSI de la organización.

4. Auditorías internas

Las auditorías internas es el proceso interno de revisión del SGSI en conformidad con la NORMA ISO 27001:2005.

La premisa de todas las auditorías, por consiguiente de todo auditor, es buscar conformidades más no no-conformidades. La ISO 27001:2005 exigen que la organización haya llevado a cabo auditorías internas y los resultados de las mismas sean revisados por la dirección. Por lo general las auditorías internas se las lleva a cabo antes de la auditoría externa y esta última se recomienda mínimo una vez al año. En nuestra implementación se las lleva a cabo cada semestre.

Mientras más exigente y formales sean las auditorías internas mayor valor agregarán a la preparación de la organización. Estas auditorías pueden ser ejecutadas por personal interno de la compañía con formación como auditores internos o en su defecto puede ser llevado a cabo por personal externo como ejemplo una empresa consultora. Lo recomendación es que sea personal interno quien realice las auditoría de una forma cruzada entre los

diferente áreas de la organización, o sea que nadie puede auditar su propia área.

Las organizaciones deben manejar programas de auditoría (cronograma general o anual), planes de auditorías (objetivos, horarios y secuencia de auditorías) y listas de chequeo (preguntas puntuales por área). Son herramientas que ayudan a las planificar, ejecutar y reportar las auditorías internas.

Dentro del informe de auditoría se debe especificar las conformidades generales o fortalezas, no conformidades, observaciones y oportunidades de mejora. La definición de cada una de ellos es la siguiente:

Las no conformidades son aquellas oposiciones a la norma que se pueden redactar con el lenguaje natural de la misma. Es decir contrario a todos los DEBES textuales de la redacción.

Las observaciones son situaciones que a pesar de no ser no-conformidades pueden transformarse en ellas, sino se les da el tratamiento debido.

Las oportunidades de mejora son los puntos en que se puede sofisticar el sistema.

4.1 Auditorías de Terceras partes.

Las auditorías de terceras partes, dentro de nuestro contexto, se refieren a las auditorías externas que pueden ser llevadas a cabo por una entidad certificadora, empresa consultora, clientes. Cada uno con sus fines específicos.

Dependiendo del tamaño de la organización la auditoría externa puede ser llevada a cabo por un equipo de auditores dirigidos por un auditor líder.

Puntos claves de Inversión.

5. Recursos necesarios

Esta norma está pensada para que cualquier empresa pueda implementarla independientemente al poder económico que ella posea.

En realidad, una mayor cantidad de recursos económicos, pueden ser diferenciadores en lo que respecta a la cantidad de tareas automatizadas que se pueden adoptar, por consiguiente la carga operativa en planear, implementar, monitorear y mejorar el SGSI es menor y más llevadero para toda la organización, a diferencia de procedimientos manuales y documentos impresos

5.1 Puntos claves de Inversión.

Se recomienda que la organización enfoque la inversión en los siguientes puntos:

- Capacitación del personal clave: manager del proyecto, miembros del equipo de trabajo.
- Mecanismos de concientización de todo el personal.
- Formación de un equipo de auditores internos.
- Formación de Auditor Líder certificado ISO 27001:2005 por IRCA.
- Pre-auditoría de diagnóstico.
- Automatización y/o elaboración de herramientas de apoyen la medición de los controles, mejoramiento continuo.
- Crear un ambiente favorable en los talleres multidisciplinario.

CONCLUSIONES Y RECOMENDACIONES.

1. La norma ISO 27001:2005 está orientada al tratamiento de la seguridad de la información mediante la gestión del riesgo, tanto para sus activos como para sus procesos. Esto garantiza que ante recursos limitados las inversiones sean bien focalizadas.

2. Hay decisiones respecto al cumplimiento de políticas dentro SGSI que deben ser de carácter jerárquico, impulsado por el director de la organización, siendo este el primer paso para adaptarse a todo cambio coyuntural dentro de la empresa.

3. Para poder tener una implantación exitosa del SGSI, los objetivos del mismo deben estar alineados al negocio de la compañía, caso contrario el valor que agrega no sería muy tangible.

4. La concientización de la compañía es un pilar fundamental de esta norma, por lo cual las organizaciones deben ingeniosamente buscar y adoptar mecanismos que permitan que se despierte un interés y compromiso por parte de todos los empleados. Existen mecanismos como bonos, viajes, cenas o reconocimientos públicos que siempre despiertan interés.

5. Las organizaciones deben tratar de hacer lo más llevadero posible las tareas operativas del sistema SGSI, para lo cual necesitan la ayuda de herramientas tecnológicas que automaticen ciertas tareas.

7. Un SGSI no puede ser implantado por moda sino siempre buscando objetivos claros que agreguen valor a la organización. Toda nueva implementación

en pro de mejoras en la seguridad de la información debe ir acompañado de políticas funcionales que direccionen los esfuerzos hacia los objetivos del SGSI

8. El tener implantado un SGSI certificado bajo la norma ISO 27001:2005 no significar contar con seguridad máxima en la información de la organización sino que esto significa que la empresa cumple con los requerimientos y mejores prácticas establecidas en dicha norma para que su SGSI actual funcione correctamente y además pueda evolucionar hacia la sofisticación.

9. El eslabón más débil de la cadena son las personas, por lo tanto dentro del análisis y evaluación del riesgo del SGSI se debe dar el énfasis necesario para considerar este tipo de amenazas. Siempre aplicando en los perfiles el principio del mínimo conocimiento.

AGRADECIMIENTOS

Agradezco a la empresa TELCONET S.A, en la cual laboro como Gerente de Seguridad de la Información por todo su apoyo y confianza para llevar a cabo este proyecto.

BIBLIOGRAFIA Y REFERENCIAS.

1. International Standard Organization, Norma ISO/IEC FDIS 27001:2005(E).
2. Alexander Alberto Ph.D , Diseño de un Sistema de Gestión de Seguridad , Editorial Alfaomega, Colombia, 2007
3. British Standard Institute , Website www.bsi.com ,