Gestionar la inseguridad para mejorar la seguridad de la información: Un marco conceptual para la medición de la inseguridad.

El verdadero objetivo de la seguridad no es eliminar la inseguridad, es enseñarnos a convivir con ella.

Richard D. García Rondón, MSc., CISSP, CISA, ABCP.

En la era actual[1], la información y en particular el conocimiento que se puede generar a partir del mismo, es reconocido [2] por la sociedad como un factor indispensable para su desarrollo. Así, el conocimiento permite a una sociedad o cualquier organización marcar una diferencia y tomar ventajas en cualquiera que sea la temática a competir. La información, entonces se convierte en un elemento estratégico y el cuidado de la misma, teniendo en cuenta sus características[2] que permitan generar un buen conocimiento, se ha convertido en uno de los desafíos más importantes hoy en día de nuestra sociedad y organizaciones que la conforman.

Afortunadamente nuestra sociedad ha ido tomado acciones [3] sobre la protección de la información, acciones que se iniciaron desde el punto de la seguridad informática, pasando por la seguridad de la información y llegando a la Gestión de la Seguridad de la Información.

Pero, ¿cuál es la diferencia entre la seguridad de la información y la gestión de la misma?, ¿cómo o cuándo una organización puede establecer que no sólo tiene seguridad de la información sino que la gestiona?

Uno de los aspectos sobre los cuales se puede marcar la diferencia entre la seguridad de la información y la gestión de la misma es el mejoramiento o evolución de ésta de acuerdo a las necesidades de la organización. De forma abreviada, gestionar la seguridad es garantizar que las medidas y controles que tenemos para proteger nuestra información son en cada momento los indicados y no sólo la apreciación en un instante de su ciclo de vida. Ya que:

- Conocemos la información de la organización y la que debemos proteger.
- Conocemos de qué la debemos proteger.
- Conocemos por qué se ha implementado cada control de protección.
- Conocemos la efectividad de los controles.

---

[1] La era en la cual nos encontramos es el tecno-capitalismo o economía intangible, en la que los cuatro recursos claves para la actividad económica y la ventaja competitiva serían: El conocimiento, colaboración, compromiso y calidad temporal. [1].

[2] Las características básicas que se consideran en la seguridad de la información son la confidencialidad, integridad y disponibilidad. Lo anterior no limita a la organización a establecer otras características relevantes a proteger para su misión.

Ahora, este mejoramiento necesario para la gestión, no puede ser realizado si no existe medición alguna sobre la temática, medición que nos permitirá determinar en que estamos fallando de acuerdo a los objetivos planteados. Pero en algo tan subjetivo como la seguridad, ¿cómo realizamos esta medición?, la medición así, se convierte en un reto en muchas ocasiones frustrante.
El presente documento tiene como objetivo plantear un marco para la medición de la gestión de la seguridad de la información, basado en la inseguridad, factor clave para determinar la efectividad de la gestión en sí misma.

Gestión de la seguridad de la información

ISO define el Sistema de Gestión de Seguridad de la Información, de ahora en adelante SGSI, como parte de un sistema de administración, que basado en un análisis de riesgo, permite la implementación, operación, monitoreo, revisión, mantenimiento y mejora de la seguridad de la información [4]. Desde luego cada una de estas acciones está orientada a proteger la información importante para el cumplimento de la misión[3], donde la misión define la razón de la existencia de la organización en si.

Los sistemas de gestión poseen actividades que están orientadas a tratar la problemática particular y otras acciones cuyo objetivo es *"Gestionar"* y/o "*permitir*" las primeras. Es así como podemos plantear entonces acciones que indudablemente se deben desarrollar, y otras, que de acuerdo a nuestras necesidades, en este caso la seguridad de la información, necesitamos implementar. Las primeras son los procesos del sistema de gestión y las segundas son los controles particulares a desarrollar de acuerdo al análisis de riesgo realizado.

De acuerdo con lo anterior podemos plantear los siguientes procesos para el SGSI[4]:

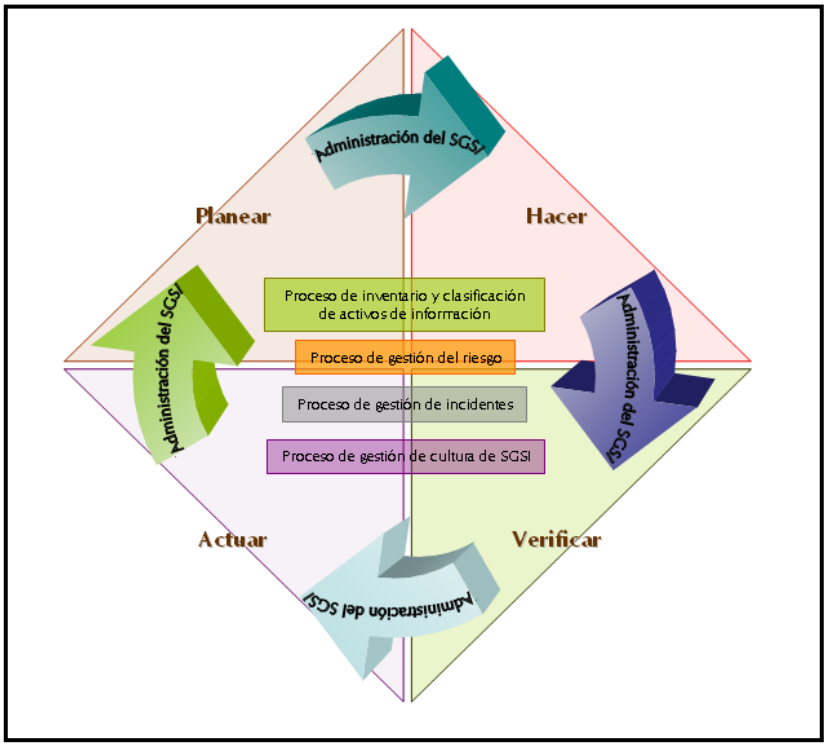
- Procesos de Administración del Sistema de Gestión (SG).
- Proceso de Inventario y clasificación de activos de información.
- Proceso de gestión del riesgo.
- Proceso de gestión de incidentes.
- Proceso de gestión de la cultura de SGSI.

¿Cuál es la razón del planteamiento anterior[5]? Debido a que se considera que, sin la existencia de cualquiera de ellos, no puede establecerse un SGSI. De igual forma podría pensarse en otros procesos como la gestión de la continuidad del negocio, pero estos son considerados como controles y no hacen parte

[3] Existen algunas organizaciones que pueden sobrevivir sin el cumplimiento de su misión.
[4] De acuerdo al estándar ISO/IEC 27001:2005.
[5] No es el tema principal de discusión del presente documento.

constitutiva del SGSI, es decir, éste (el SGSI) puede existir sin contar con él[6], por el contrario no lo podría hacer sin un proceso de inventario y clasificación de activos, el cual indica qué información se debe proteger y cómo se debe tratar.

A continuación se describen muy brevemente estos procesos.
Proceso de administración del SG: Dentro de este proceso se encuentran aquellas actividades propias del sistema de gestión, entre estás se encuentran: el control de la documentación y registros, la revisión del SG por parte de la dirección o gerencia de la organización, la definición de las responsabilidades, las acciones correctivas y preventivas y las auditorias al SG entre otras. Estas actividades son similares en cualquier sistema de gestión independiente del tema que éste maneje, es por esta razón que es plasmado alrededor de los demás procesos, ya que es éste el que permite la gestión (alineado al PHVA) de los procesos particulares a la seguridad de la información. Ahora, una vez que la organización haya puesto en marcha este proceso con cualquier temática particular[7], incluir una nueva será mucho más fácil. Ver gráfica No 1.



[6] Un SGSI puede existir sin un proceso de gestión de continuidad del negocio, pero debe ser claramente justificada la no necesidad del mismo.
[7] 9000, Gestión de Calidad; 14000, Gestión Ambiental; 1800, Salud Ocupacional y Seguridad Laboral; 27000, Gestión de la Seguridad de la Información, entre otras.

Gráfica No 1. Procesos del Sistema de Gestión de la Seguridad de la Información.

Proceso de inventario y clasificación de activos de información: En este proceso se requiere identificar, valorar y clasificar los activos de información más importantes del negocio y así darles el tratamiento adecuado. Un activo de información en el contexto de un SGSI y con base en la norma ISO/IEC 27001:2005 es: "algo a lo que una organización directamente le asigna un valor y por lo tanto la organización debe proteger" [5].

Proceso de gestión del riesgo: El proceso de gestión del riesgo consiste en la definición de una metodología para su manejo, una identificación del riesgo, un análisis del riesgo y un plan para el tratamiento del mismo que permita disminuir su nivel a un estado aceptable. Dentro del plan para el tratamiento de riesgo se plantean los controles que llevarán el riesgo al nivel deseado, y es así como en este proceso se incluye la gestión de éstos[8].

Proceso de gestión de incidentes: El objetivo principal de este proceso es definir acciones que permitan manejar adecuadamente los incidentes[9] a través de un esquema que involucra actividades de manera cíclica: preparación, detección y análisis, contención y actividades post incidentes para evitar la ocurrencia nuevamente del incidente. [6]. Este proceso es fundamental para la medición de la efectividad de los controles implementados siempre y cuando los incidentes sean relacionados con los controles que debieron impedir su ocurrencia.

Proceso de gestión de la cultura de SGSI: El proceso de gestión de la cultura provee el conocimiento acerca de la seguridad de información, a medida que el personal progresa en el desarrollo de la cultura, la necesidad de la misma es interiorizada y su rol es desarrollado. Así, al desarrollar el rol, el personal comienza a actuar de forma más segura y a utilizar las medidas implementadas. Dentro del proceso se incluyen etapas como: sensibilización, entendimiento y uso efectivo de las medidas.

Es recomendable que el proceso de administración del SG, aquel que permite que el sistema de gestión gire, sea introducido dentro de la empresa como un proceso en sí, con un flujo bien determinado, actividades, actores y responsabilidades acordes ya que forma en si la verdadera gestión de un sistema basado en el PHVA[10] el cual garantiza el monitoreo, la medición de resultados, y la definición e implementación de la mejoras. La existencia de este proceso en la organización

[8] Aspecto clave para la definición del marco conceptual para los indicadores de gestión del SGSI a describir más adelante.
[9] Incidente de seguridad de la información está indicado por un evento o serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. [5].
[10] ISO avoca a las cuatro fases para el establecimiento de un SGSI, PHVA: Planear, Hacer, Verificar y Actuar. [4].

facilita la inclusión de nuevos sistemas de gestión sin la necesidad de crear nuevas actividades.

Los demás procesos planteados, que caracterizan un SGSI, se deben definir de igual manera con sus actividades, actores y responsabilidades. Pero a diferencia del anterior, es recomendable que estos procesos se introduzcan dentro de las funciones ya existentes en la organización, ya que es primordial no generar actividades extras de seguridad sino hacer las actividades del negocio de forma segura, de esta manera el impacto de la inclusión de un SGSI en la organización se lleva al mínimo.

Planteamiento de un marco conceptual para la medición de la inseguridad en un sgsi

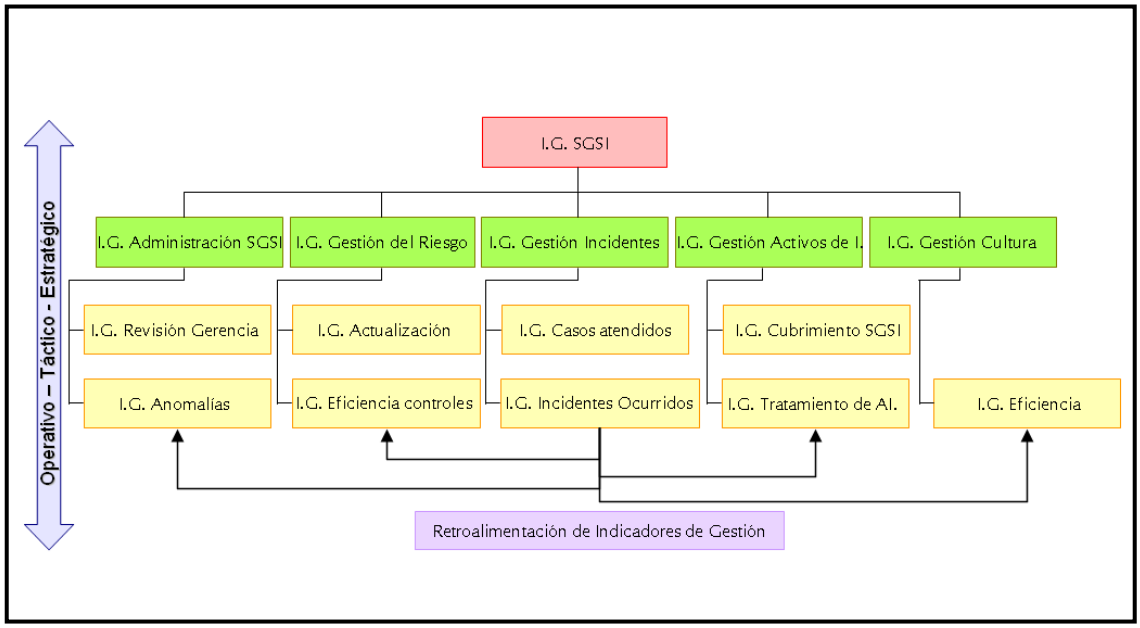
"No todo lo que puede ser contado cuenta,
y no todo lo que cuenta puede ser contado".
Albert Einstein.

La pregunta del millón es entonces ¿Qué puede ser contado que cuente? Una vez definido en el apartado anterior un marco de gestión es relativamente sencillo abordar un marco para la medición de esta gestión. Algo recomendable es utilizar la misma estructura, tanto para la gestión como para su medición, esto obviamente nos permite establecer una relación directa en "Como lo hago, lo mido".

Así se genera una estructura de Indicadores de Gestión, IGs[11], (ver gráfica No 2), que van desde los aspectos operativos, abordando los tácticos y alimentado los estratégicos, éstos últimos la razón de ser del marco de gestión. El primer nivel, *I.G. SGSI*, el nivel estratégico, define los IGs que se desprenden de los objetivos a alcanzar en un periodo de medición, estos determinarán cuáles son los IGs relevantes a nivel táctico y operativo. Los IGs de color verde, el segundo nivel, enmarcan cada uno de los procesos planteados como indispensables dentro del SGSI, de esta manera cada aspecto puede llegar a ser medido. Como se mencionó anteriormente los diferentes controles y desde luego su medición, se encuentran dentro de la gestión del riesgo.

Los IGs de color amarillo, nivel operativo, son aquellos encargados de alimentar todo el marco ya que definen la medición particular a realizar.

[11] De ahora en adelante IG.



Gráfica No 2. Marco conceptual para la medición de la inseguridad en un SGSI.

En este instante podría entrar una segunda pregunta al escenario ¿Por qué definir un marco, si lo interesante debería llegar a ser los indicadores en sí mismos? Los indicadores de gestión deben ser enmarcados de acuerdo a las políticas y objetivos de la organización y de la seguridad de la información, no pueden ser estáticos, ni establecidos de forma unilateral por algún área, pues así no medirán lo que se desea realmente mejorar.

Es así, como los IGs para la medición de la gestión de la seguridad de la información deben definirse partiendo de lo que la organización desea evolucionar o mejorar en un lapso de medición determinado, y de esta manera apoyarán la consecución de los objetivos propuestos.

Por ejemplo, si una organización plantea como objetivo el mejoramiento de la cultura organizacional en el tema de seguridad de la información, indicadores adecuados para la medición del cumplimiento de este objetivo serían: el número del personal capacitado sobre el personal total; la eficiencia de las capacitaciones y el número de incidentes de seguridad relacionados con la falta de cultura de seguridad, entre otros. Por el contrario IGs como el cubrimiento a los procesos por parte del SGSI o el número de revisiones realizadas por la dirección no nos sería de mucha ayuda en el seguimiento y mejora para la consecución del objetivo planteado.

Ahora, lo anterior no pretende expresar que estos otros IGs no sean útiles, de hecho lo son, pero se desea hacer énfasis en medir lo que realmente nos interesa, buscando el enfoque y visualización de los objetivos planteados y así no quedar inmersos en la información misma.

¿Cuál es el papel que juega la inseguridad en este planteamiento? Partiendo de la problemática descrita en [7] en la cual la seguridad posee un gran componente subjetivo ya que es percepción propia de cada sujeto lo que la convierte en algo complejo para su medición, la inseguridad se convierte en candidata importante debido a su objetividad, al ser una realidad perceptible, observable y verificable, siendo en sí la fuente misma para el análisis de riesgo del cual se desprenden los controles a desarrollar [7].

Complementando y de acuerdo a lo planteado en este artículo, ¿Cuál sería el proceso que puede proveer información de inseguridad en un SGSI?: el proceso de gestión de incidentes. Es así como este proceso es tan importante en nuestro SGSI, ya que suministra la información prioritaria que permite el mejoramiento en el sistema. Al relacionar cada incidente con la temática afectada, se puede retroalimentar (ver gráfica No 2) la forma como se están ejecutando los procesos básicos y mejor aún determinar la eficiencia de los controles[12] implementados ya que se puede establecer cuáles de ellos fallaron (y cómo lo hicieron) y permitieron la ocurrencia de un incidente.

Con la implementación de un proceso de gestión de incidentes[13] con sus IGs gestionamos la inseguridad, retroalimentado los procesos constitutivos del SGSI y sus IGs con la información de inseguridad, gestionamos la seguridad de la información.

Conclusiones

En el momento que una organización decide emprender el cambio de tener seguridad de la información a gestionarla, debe afrontar varios retos dentro de los cuales se encuentra la medición de la eficiencia de sus acciones en torno a la seguridad con el objeto de garantizar un verdadero mejoramiento, y así una gestión que no se quede sólo en el papel. La medición de la seguridad se convierte en un reto cada vez mayor debido a lo dinámica de la misma y a su alto grado de subjetividad. En este escenario nada alentador el concepto de inseguridad llega al rescate, permitiendo, desde un punto de vista más objetivo, obtener información relevante, medible, que permite retroalimentar los procesos constitutivos de un Sistema de Gestión de la Seguridad de la Información y generar una mejora que se puede evidenciar. Para lograr lo anterior se plantea entonces un marco conceptual para medir la inseguridad a través del proceso de gestión de incidentes y a la vez retroalimentar los procesos de seguridad con lo

[12] Aspecto importante a la hora de la implementación y certificación de un SGSI bajo la norma ISO/IEC 27001:2005.
[13] "Gestión" de Incidentes se entiende como un proceso que se encuentra inmerso dentro de un SGSI y así puede mejorar.

cual se puede determinar las falencias existentes y las mejoras a desarrollar, produciéndose así, la anhelada gestión.

Referencias

[1] Era de la información. http://es.wikipedia.org/wiki/Era_de_la_informaci%C3%B3n.
[2] Plan Nacional de tecnologías de la Información y las Comunicaciones. http://www.colombiaplantic.org.
[3] VII Encuesta Nacional de Seguridad Informática http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VII_JornadaSeguridad/VIIENSI.pdf.
[4] Willett, K.; How to Achieve 27001 certification. An Example of Applied Compliance Management. USA, 2008.
[5] ISO/IEC 27001:2005.
[6] Cárdenas, F.; Gestiones de Seguridad de la Información en las Organizaciones. 2007.
[7] Cano, J.; Inseguridad Informática y Computación Anti-forense: Dos Conceptos Emergentes en Seguridad de la Información. ISACA 2007. www.isaca.org.

Richard D. García Rondón. *Ingeniero Naval "especialidad electrónica" – Escuela Naval Almirante Padilla. Especialista en servicios telemáticos – Fundación Caixa Galicia - Universidad de la Coruña. Magíster en Ingeniería de Sistemas y Computación – Universidad de los Andes. CISSP, CISA, ABCP, LA BS 27001 ISO/IEC 27001:2005. Consultor Senior en Seguridad de la Información. richardgarcia@hotmail.co.uk.*