Eficiencia Gerencial y Productividad S. A.
Pedro Irigoyen 116, Miraflores
Lima - Perδ
Telf. (511) 4343528 Fax: (511) 4366144

Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El Enfoque ISO 27001:2005

Por

Alberto G. Alexander, Ph.D
Auditor SGSI Certificado IRCA
alexander@eficienciagerencial.com
www.eficienciagerencial.com

Introducción.-

El propósito de la seguridad de información es asegurar la continuidad del negocio y minimizar daños a la firma previniendo y minimizando el impacto de incidentes de seguridad. La gestión de seguridad de información permite que la información sea compartida, asegurando la protección de la información y todos los activos comprendidos en el alcance del sistema.
Un sistema de gestión de seguridad de información (SGSI) tiene tres componentes para alcanzar confidencialidad y aseguramiento de la información:

- Confidencialidad: protección de la información sensitiva de intercepciones no autorizadas.
- Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos.
- Disponibilidad: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada si se desea ser utilizado para la certificación.
-

El 15 de Octubre del 2005 nació un nuevo estándar, y el BS 7799 fue reemplazado. El nuevo modelo es el ISO 27001:2005. Es el único estándar para ser utilizado para la implantación de un SGSI y si se desea, aplicarlo para propósitos de certificación de una organización o parte de ella, de acuerdo al alcance del estándar.
La gestión del riesgo es una parte esencial del ISO 27001:2005. Los controles en el anexo A del estándar debieran ser seleccionados en base a los resultados de la evaluación del riesgo y a las decisiones tomadas concernientes al tratamiento del riesgo. Las organizaciones que acuden a una certificación de tercera parte, basadas en el ISO 27001:2005, requieren medir y evaluar los riesgos así como revisar y reevaluar los riesgos en una etapa futura para asegurar que se tiene implantado una eficaz seguridad de información. Los requerimientos de las revisiones gerenciales explícitas en el estándar, están basadas en retroalimentación recibida del proceso de gestión del riesgo.

Los controles de gobierno empresarial están basados en el proceso de gestión del riesgo. Sin estar bien informados sobre los riesgos una empresa no puede alcanzar una efectiva gestión de control.
En lo que resta del artículo, el autor tocará una serie de aspectos relacionados con el proceso de la evaluación del riesgo desde la perspectiva del ISO 27001:2005.

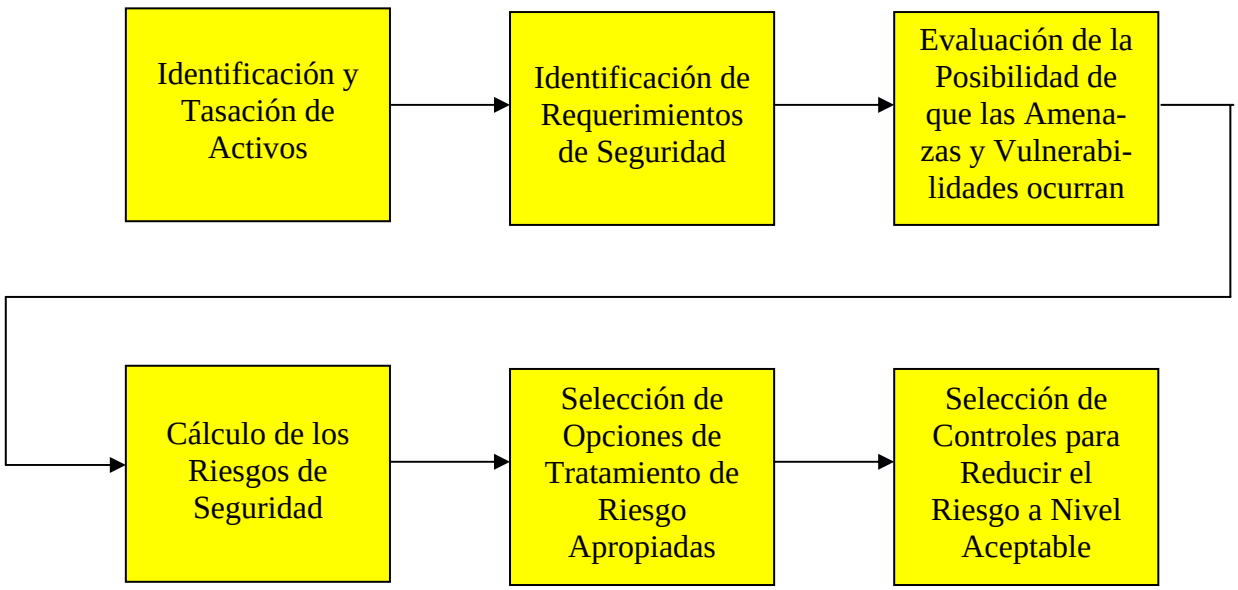
Análisis del Riesgo y los Requerimientos del ISO 27001:2005

El ISO 27001:2005 requiere que la organización que esta planeando implantar un SGSI, que primero defina el alcance del estándar en la empresa, y en base a ese alcance identificar todos los activos de información. Los activos de información deben ser tasados para identificar su impacto en la organización. Luego un análisis del riesgo es requerido para determinar que activos están bajo riesgo. “Se deben tomar decisiones en relación a que riesgos la organización aceptará y que controles serán implantados para mitigar el riesgo” (Alberts, Dorofeee, 2003) A la gerencia se le requiere que revise el SGSI en la organización a intervalos planificados para asegurar su adecuación y eficacia. La gerencia es exigida que controle los niveles de riesgos aceptados y el estado del riesgo residual (riesgo que queda después del tratamiento del riesgo). El ISO 27001:2005 es un sistema dinámico que obliga a la gerencia estar constantemente revisando y definiendo controles, sus amenazas, vulnerabilidades e iniciar acción correctiva y preventiva cuando sea necesario.

Proceso de Evaluación del Riesgo

El proceso de evaluación del riesgo que permite a una organización estar en conformidad con los requerimientos del estándar esta presentada en la figura N° 1. El proceso de las seis fases ayuda a cualquier organización que desee establecer un SGSI, en concordancia con la cláusula 4.2.1 del estándar. En los siguientes párrafos una breve descripción de las fases del proceso de evaluación del riesgo será hecho para permitir a las organizaciones gestionar adecuadamente el proceso de evaluación del riesgo al implantar el estándar.

Figura Nº 1: Proceso de Evaluación del Riesgo



Identificación y Tasación de Activos.- Un activo es algo que tiene valor o utilidad para la organización, sus operaciones y su continuidad. Los activos necesitan protección para asegurar las correctas operaciones del negocio y la continuidad de la empresa. "La gestión apropiada de los activos es vital para poder mantener una adecuada protección de los activos de la empresa." (Peltier, 2001)

Cada activo debe estar claramente identificado y valorado apropiadamente, y su propietario y clasificación de seguridad acordada en la organización. El ISO 17799:2005 (Código de Práctica para la Gestión de la Seguridad de Información) clasifica los activos de la siguiente manera: **(1)** Activos de información: bases de datos y archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo, planes de continuidad, **(2)** Documentos impresos: documentos impresos, contratos, lineamientos, documentos de la compañía, documentos que contienen resultados importantes del negocio, **(3)** Activos de software: Software de aplicación, software de sistemas, herramientas de desarrollo, **(4)** Activos físicos: Equipos de comunicación y computación, medios magnéticos, otros equipos técnicos, **(5)** Personas: Personal, clientes, suscriptores, **(6)** Imagen y reputación de la compañía, **(7)** Servicios: Servicios de computación y comunicación, otros servicios técnicos.

La tasación de activos, basados en las necesidades del negocio de una organización, es un factor importante en la evaluación del riesgo. Para poder encontrar la protección apropiada para los activos, es necesario evaluar su valor en términos de su importancia para el negocio. "Para poder tasar los valores de los activos y poder relacionarlos apropiadamente, una escala de valor para activos debe ser aplicada." (Alberts, Dorofee, 2003)

Identificación de Requerimientos de Seguridad Los requerimientos de seguridad en cualquier organización, grande o pequeña, son derivados de tres fuentes esenciales y debieran de documentarse en un SGSI.

- El conjunto único de amenazas y vulnerabilidades que pudieran ocasionar pérdidas significativas en la empresa si ocurrieran.
- Los requerimientos contractuales que deben satisfacerse por la organización.
- El conjunto único de principios, objetivos y requerimientos para el procesamiento de información que una organización ha desarrollado para apoyar las operaciones del negocio y sus procesos.

Una vez que estos requerimientos de seguridad han sido identificados, es recomendable formularlos en términos de requerimientos de confidencialidad, integridad y disponibilidad.

Identificación de Amenazas y Vulnerabilidades Los activos están sujetos a muchos tipos de amenazas. Una amenaza tiene el potencial de causar un incidente no deseado, el cual puede generar daño al sistema, la organización y a los activos. El daño puede ocurrir por un ataque directo o indirecto a la información organizacional. Las amenazas pueden originarse de fuentes accidentales o de manera deliberada. Una amenaza para poder causar daño al activo, tendría que explotar la vulnerabilidad del sistema, aplicación o servicio.

Las vulnerabilidades son debilidades asociadas con los activos organizacionales. Las debilidades pueden ser explotadas por la amenaza, causando incidentes no deseados, que pudieran terminar causando pérdidas, daño o deterioro a los activos. La

vulnerabilidad como tal, no causa daño, es simplemente una condición o conjunto de condiciones que pueden permitir que una amenaza afecte a un activo. Una evaluación de la posibilidad de ocurrencia de las vulnerabilidades y las amenazas, debe ser efectuada en esta fase.

Cálculo de los Riesgos de Seguridad El objetivo de la evaluación del riesgo es la de identificar y evaluar los riesgos. Los riesgos son calculados de una combinación de valores de activos y niveles de requerimientos de seguridad.
La evaluación de riesgos envuelve la sistemática consideración de los siguientes aspectos:

- Consecuencias.- El daño al negocio como resultado de un incumplimiento de seguridad de información considerando las potenciales consecuencias de pérdidas o fallas de confidencialidad, integridad y disponibilidad de información.
- Probabilidad.- La real posibilidad de que tal incumplimiento ocurra a la luz del reinado de amenazas, vulnerabilidades y controles.

Es importante hacer hincapié que no existe una manera "buena" o "mala" de calcular los riesgos, en la medida que los conceptos descritos en las fases anteriores se combinen en una manera sensata. Es menester de la firma identificar un método para la evaluación del riesgo que sea adecuada a los requerimientos de seguridad del negocio.

Selección de Opciones Apropiadas de Tratamiento del Riesgo Cuando los riesgos han sido identificados y evaluados, la próxima tarea para la organización es identificar y evaluar la acción más apropiada de cómo tratar los riesgos. La decisión debe ser tomada basada en los activos involucrados y sus impactos en el negocio. Otro aspecto importante ha considerar es el nivel de riesgo aceptable que ha sido identificado siguiendo la selección de la metodología apropiada de evaluación.
El estándar ISO 27001:2005, requiere que la organización en relación al tratamiento del riesgo siga cuatro posibles acciones:

- Aplicación de apropiados controles para reducir los riesgos. Los controles tienen que ser identificados en el anexo A. Si los controles no pueden ser hallados en el anexo A, la firma puede crearlos y documentarlos.
- Aceptar objetivamente los riesgos partiendo del supuesto que satisfacen la política de la organización y su criterio para la aceptación del riesgo.
- Evitar los riesgos
- Transferir el riesgo asociado a otras partes.

La organización por cada uno de los riesgos, debe evaluar estas opciones para identificar la más adecuada. Los resultados de esta actividad deben ser documentados y luego la firma debe documentar su "plan de tratamiento del riesgo".
Hay dos opciones en la identificación y evaluación del riesgo que requieren mayor explicación. Las alternativas son: "evitar el riesgo" y "transferencia del riesgo". **(a)** Evitar el riesgo. Describe cualquier acción donde los activos son transferidos de las áreas riesgosas. Cuando se evalúa la posibilidad de "evitar el riesgo" esto debe sopesarse entre las necesidades de la empresa y las monetarias. **(b)** Transferencia del riesgo. Esta opción puede ser vista como la mejor si es imposible reducir los niveles del riesgo. Existen muchas alternativas a considerar en relación a la estrategia de transferencia del riesgo. La transferencia del riesgo podría alcanzarse tomándose una póliza de seguro. Otra posibilidad podría ser la utilización de servicios de "outsourcing"

para que se manejen activos y procesos críticos. La responsabilidad por los servicios tercerizados siempre recae en la empresa. Eso jamás se delega.

Selección de Controles para Reducir los Riesgos a un Nivel Aceptable Para reducir el riesgo evaluado dentro del alcance del SGSI considerado, controles de seguridad apropiados y justificados deben ser identificados y seleccionados. Estos controles deben ser seleccionados del anexo A del ISO 27001:2005. El estándar presenta 11 cláusulas, 39 objetivos de control y 133 controles específicos. Es muy importante estar claros sobre el rol del ISO 17799:2005. La organización puede utilizar el ISO 17799:2005 como guía para la implementación de los controles, pero deben ser escogidos del ISO 27001:2005.
La selección de los controles debe ser sustentada por los resultados de la evaluación del riesgo. Las vulnerabilidades con las amenazas asociadas indican donde la protección pudiera ser requerida y que forma debe tener. Especialmente para propósitos de certificación, las relaciones con la evaluación del riesgo deben ser documentadas para justificar la selección de los controles.
Cuando se seleccionan controles para la implementación, un número de factores deben ser considerados, incluyendo:

- Uso de controles
- Transparencia del usuario
- Ayuda otorgada a los usuarios para desempeñar su función
- Relativa fuerza de los controles
- Tipos de funciones desempeñadas.

En términos generales, un control podrá satisfacer más de una de estas funciones y lo más que pueda satisfacer mejor.

Reducción del Riesgo y su Aceptación Para todos aquellos riesgos donde la decisión de "reducción de riesgo" ha sido escogida, controles apropiados deben ser seleccionados para reducir los riesgos a un nivel que la gerencia, de acuerdo a la cláusula del estándar 5.1 (f) decidirá su nivel adecuado.

Riesgo Residual Después de identificar los controles adecuados para reducir un riesgo específico al nivel considerado aceptable, debe evaluarse cuanto los controles, si se implementan reducirán el riesgo. Esta reducción de riesgo es el denominado "riesgo residual".
El riesgo residual usualmente es difícil evaluarlo. Por lo menos una estimación de cuanto los controles reducen el nivel de los requerimientos de los valores asociados de seguridad debieran ser identificados para asegurar que la suficiente protección es alcanzada." (Peltier, 2001)
Si el riesgo residual es inaceptable, una decisión comercial debe ser tomada sobre como se irá a manejar la situación. Una opción es la de seleccionar mas controles para finalmente reducir los riesgos a un nivel aceptable. Es una buena práctica no tolerar riesgos inaceptables, pero muchas veces no es posible o financieramente factible reducir todos los riesgos al nivel aceptable.
Después de la implementación de los controles seleccionados, es importante estar claros, que siempre habrá riesgos existentes. Esto sucede por que los sistemas de información en las organizaciones nunca podrán estar absolutamente seguros. Esta es la razón por la cual es necesario revisar la implementación, y los resultados de los controles para finalmente evaluar qué tan bien los controles implementados están operando. Este es fundamentalmente el propósito de las "revisiones gerenciales" para

poder tener un control concreto del proceso del riesgo en la firma y poder iniciar la acción correctiva cuando sea necesario.

Conclusiones

La implementación del ISO 27001:2005 dentro de cierto alcance previamente determinado en la empresa, tiene un requerimiento básico, el cual es una completa participación de la gerencia. Este estándar es un sistema de gestión. Esta hecho para gestionar un sistema de seguridad de información. Su propósito fundamental es el de asegurar que la información en la firma mantenga: confidencialidad, integridad y disponibilidad.
La gestión del riesgo es el tema central de este nuevo estándar internacional. Un antiguo axioma plantea que uno no puede mejorar lo que no se puede medir. Esto es cierto para la gestión del riesgo. Uno no puede gestionar el riesgo si no se puede medirlo.
La dinámica de este nuevo estándar es bien clara en términos de mitigar la información del riesgo en la empresa. La firma tiene la autonomía de decidir el alcance del estándar. Luego tiene que identificar los activos dentro del alcance y realizar por cada activo de información un análisis y evaluación del riesgo para determinar el plan de tratamiento del riesgo. Esos activos que tendrán apropiados controles para reducir los riesgos serán escogidos del anexo A del estándar. El ISO 17799:2005 provee sólo información como guía para la implementación de los controles. Es importante estar claros que los controles del anexo A no son exhaustivos y controles adicionales podrán diseñarse si se requieren.
Considerando el proceso de globalización y las nuevas reglas del comercio internacional, las organizaciones para poder penetrar nuevos mercados y poder demostrar confianza en la cadena de suministros, tendrán que implementar el ISO 27001:2005. El estándar se esta convirtiendo en un requerimiento en los mercados internacionales.

Referencias Bibliográficas

(1) Alberts, Christopher, Dorofee, Autrey. Managing Information Security Risks. Peaerson Education. 2003. Boston
(2) Peltier, Thomas. Information Security Risk Analysis. Auerbach. 2001 London.