De los estándares, marcos de trabajo, normas y la seguridad de la información.

Aponte Buitrago, Juan de Jesús
jjabtecno@gmail.com
Universidad Piloto de Colombia

Resumen — Este artículo pretende dar una visión de la importancia que ha cobrado la seguridad de la información, la inclusión de esta en estándares, marcos de trabajo y normas, revisando el desarrollo que ha tenido a través de los años, y la integración con los procesos de las empresas.

Abstract — This article to provide a vision that the importance which has taken the information security, the inclusion of that in standards, frameworks, and norms, review the envelopment that it had along the years and the integration with process of the company.

Índice de Términos—*SEGURIDAD-INFORMACIÓN-ISO-ITIL-COBIT-PMP*.

I. INTRODUCCIÓN

La evolución de las empresas, sus procesos, su forma de gestión, y aún más importante la evolución de la información, las nuevas formas de generación, almacenamiento y transmisión, traen consigo cambios en la manera como se gestiona, se protege y se visualizan los riesgos inherentes a esta.

Pero también tienen que evolucionar las normas, estándares y marcos de trabajo, para estar alineadas con esos cambios acelerados que tiene el ciclo de la información gracias a la tecnología y más aun con la preocupación creciente por la seguridad de la misma, por ese esfuerzo de proteger la información desde su origen hasta su destrucción.

Estas normas, estándares y marcos de trabajo han venido incluyendo de manera progresiva la seguridad de la información como parte fundamental de sus actividades, estableciendo modelos y puntos de partida para la implementación de seguridad en la información.

Entre las normas, estándares y marcos de trabajo que hacen referencia a seguridad de la información encontramos, circular 052 de la superintendencia financiera de Colombia, Ley 1581 de 2012, decreto 1373 de 2013, ISO 27001, COBIT, ITIL.

Estas y otras dan parámetros, ideas, modelos que pueden ayudar a las empresas a implementar sistemas de gestión de seguridad y proteger su información.

II. ¿POR DÓNDE COMENZAR?

Cuando hablamos de la implementación de seguridad en la información surgen varias incógnitas: ¿por dónde comenzar?, ¿qué debo realizar primero?, ¿cómo afronto este nuevo reto?.

Y comenzamos a consultar infinidad de información en libros, artículos, cursos y páginas especializadas y nos encontramos con los análisis de brecha, los análisis de riesgos, la creación de políticas, etc., llevándonos a un conglomerado de tareas y actividades que muchas veces se realizan en forma desordenada conduciendo a un desajuste entre los resultados esperados y los obtenidos, gastando más tiempo y recursos de los presupuestados lo que vuelve casi infinita la implementación del Sistema de Gestión de Seguridad de la Información.

Y si utilizamos lo que ya está hecho y comprobado para realizar una implementación de seguridad de la información de una forma ordenada y clara,

guiándonos en la norma ISO 27001 la cual nos entregará los requisitos para la implementación del Sistema de Gestión de Seguridad de la Información, pero no nos entregará un esquema de trabajo, solo nos dirá que debemos hacer, y tendremos que entrar a planear y diseñar todo el proceso de implementación y como controlar su ejecución, podemos asumir esta implementación como un proyecto para la organización mediante el uso de las técnicas propuestas por el Project Managment Institute en el PMBook, con lo cual nos permitirá establecer fechas de inicio y cierre, recursos necesarios, hitos, realizar una adecuada gestión del tiempo, la calidad, el recurso humano, la comunicación, los riesgos, compras y los interesados del proyecto.

III. APOYÁNDONOS EN EL PMP

Un Sistema de Gestión de Seguridad de la Información no puede ser algo eterno, aunque queda en un ciclo de mejoramiento continuo debe ponerse fin a su implementación en algún momento y pasarlo a ser parte de la operación normal dentro de la empresa. Es allí donde el PMP nos realizara una gran contribución al tratar la implantación del Sistema de Gestión de Seguridad de la Información como un proyecto, dándonos un propósito único, una fecha de inicio y fin, un patrocinador (recursos), y permitiéndonos gestionar el riesgo del mismo.

El PMBOK® Guide 4ed define un proyecto como: "Un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único", aunque un Sistema de Gestión de Seguridad de la Información se construye como un ciclo donde se planea, ejecuta, revisa, y mejora, debemos establecer un fin, un alcance para del cumplimiento del mismo poder realizar las acciones de dicho ciclo.

1) Metodología de Gestión de Proyectos. Imagen tomada del sitio Business Solutions & Technologies: http://bs-t.com.co/bst_servicios.php

Este modelo se basa en una serie de buenas prácticas divididas en 9 áreas de conocimiento, subdivididas cada una en actividades (44 en total).

Dicho modelo nos brinda un marco de trabajo para gestionar cada aspecto de un proyecto: desde gestión del alcance hasta gestión de las adquisiciones.

El PMBOK® nos entrega una referencia para establecer la base del proyecto de implementación de un Sistema de Gestión de Seguridad de la Información, para poder presupuestar su costo, las actividades a realizar, los recursos necesarios, así como para controlar los mismos, entre otras herramientas que nos serán de utilidad en nuestro proyecto del Sistema de Gestión de Seguridad de la Información como veremos en el desarrollo de este artículo.

Uno de las principales claves de éxito en la implementación de un Sistema de Gestión de Seguridad de la Información es el apoyo de la dirección, para esto se le debe suministrar a la misma la información correcta en el momento justo para la toma acertada y adecuada de decisiones.

Este apoyo de bebe ser demostrado de acuerdo al numeral 5.1 Liderazgo y compromiso, "La alta

dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información" [1].

Una forma fácil y convincente hacer evidente este apoyo es mediante el acta de constitución del proyecto. "El acta que autoriza de manera formal un proyecto o fase de un proyecto y contiene en ella los requisitos iniciales." [2]

Porqué es importante el acta de constitución para el Sistema de Gestión de Seguridad de la Información, al firmar el acta el Sistema toma mayor relevancia y se produce el primer punto para constituirlo en un proyecto, ya que con este documento se establece formalmente, se describen los requisitos iniciales, y lo más importante, el patrocinador manifiesta la disposición de recursos y herramientas para llevarlo a cabo.

El PMP también nos ayuda en un punto clave y es identificar a los interesados, a menudo las personas implicadas en un Sistema de Gestión de Seguridad de la Información se van requiriendo o incluyendo a medida que el sistema va avanzando de una forma desordenada lo cual trae consigo repercusiones en el tiempo, los recursos y los procesos, ya que son llamados a destiempo a veces sin el conocimiento previo de la implementación del sistema y con una absoluta resistencia hacia el mismo ya que pueden ser abordados cuando tenían proyectadas otras actividades o por el simple hecho de no ser tenidos en cuenta desde el principio.

Este inconveniente lo podemos abordar desde la gestión del Recurso Humano y la Gestión de las Comunicaciones en PMP. Como es conocido la implementación del Sistema de Gestión de Seguridad de la Información no solo le corresponde al área de IT, sino que es un esfuerzo y un compromiso de todos los miembros de la organización incluso los terceros que tengan una relación contractual con esta. Cuando identificamos todos los interesados, y la manera en que interactúan con el proyecto de implementación del Sistema de Gestión de Seguridad de la Información, conoceremos en que momento interactuaran con el mismo, las responsabilidades, actividades que deben desarrollar, y lograremos involucrarlos fácilmente en el proyecto ya que no serán tomados por sorpresa cuando se les requiera.

Por otro lado la gestión de las comunicaciones nos permitirá no solo tener informados a todos los implicados con el proyecto del Sistema de Gestión de Seguridad de la Información, sino retroalimentarnos sobre el mismo, y establecer como lo indica la norma ISO-IEC 27001:2013: La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al Sistema de Gestión de Seguridad de la Información, que incluyan:

a) El contenido de la comunicación
b) Cuándo comunicar
c) A quién comunicar
d) Quién debe comunicar
e) Los procesos para llevar a cabo la comunicación.

Dejando una base que nos servirá para una parte indispensable dentro del Sistema de Gestión de Seguridad de la Información que es la sensibilización y concientización en seguridad de la información a todas las personas implicadas, además de tener al tanto de cómo avanza el Sistema de Gestión de Seguridad de la Información, no solo en su fase de proyecto, sino como producto o servicio en operación.

[1] ISO-IEC 27001:2013
[2] Preparación para el examen de certificación PMP- Sandra Mercado 4ed

IV. COBIT Y EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Ya vimos de manera general como con PMP podemos iniciar la implementación de nuestro Sistema de Gestión de Seguridad de la Información como un proyecto, ahora tenemos que empezar a desarrollar el mismo y a gestionarlo no solo en su etapa de proyecto, sino cuando se entregue como un producto o servicio.

2) Áreas de Enfoque del Gobierno TI. Imagen tomada de COBIT 5® 2012. IT Governance Institute.

Aunque la seguridad de la información no está relacionada 100% con tecnología, si depende en gran medida de la misma, ya que la mayoría de datos se generar, modifican y/o almacenan en dispositivos tecnológicos y los mismos apoyan un alto porcentaje de los procesos de las empresas, encontrando así un campo adyacente conocido como seguridad de la informática.

En este caso COBIT® nos servirá como marco de trabajo para el gobierno de TI, y sobre todo como indicador del nivel de madurez de cada uno de sus procesos, consiguiendo mediante este medir y controlar todos los aspectos relacionados con la seguridad de la informática.

Aunque todo el marco de trabajo de COBIT® está orientado al gobierno de TI, dos de sus procesos nos dan un claro ejemplo de la ayuda que nos puede brindar este marco de trabajo en temas de seguridad de la información, hablamos específicamente del proceso DS4 Garantizar la Continuidad del Servicio y el DS5 Garantizar la Seguridad de los Sistemas.

En el primero DS4 Garantizar la Continuidad del Servicio, nos habla de la necesidad de implementar planes de continuidad para TI, respaldos de la información, y entrenamiento periódico. Esto lo vemos reflejado cuando implementamos en un Sistema de Gestión de Seguridad de la Información el desarrollo del Plan de Recuperación de Desastres, donde se desarrollan planes para minimizar la probabilidad de interrupciones en los servicios de TI.

En el DS5 Garantizar la Seguridad de los Sistemas, aunque es un proceso pequeño en comparación con la Norma ISO 27001 se percibe como un resumen del mismo, tomando partes importantes como base para su desarrollo, este nos habla de la necesidad de mantener la integridad de la información, de proteger los activos de TI, de la creación de políticas, procedimiento, el establecimiento roles y responsabilidades, la realización de monitoreos y pruebas a los controles y la gestión de incidentes de seguridad identificados; estos y otros componentes mencionados en este proceso de COBIT® hacen referencia a la seguridad lógica, seguridad física, seguridad de las comunicaciones y en general a la seguridad de la información.

Vemos entonces como se alinea COBIT® e ISO 27000 en estos aspectos permitiendo implementar ambos marcos de trabajo de manera simultánea sin realizar reprocesos o doble trabajo, haciendo más eficientes las tareas realizadas en el desarrollo de los mismos.

COBIT® no desarrolla el plan de continuidad del servicio, pero si entrega herramientas que son de gran ayuda para establecer lo que debe contener este plan, los controles a implementar, las metas a alcanzar, las métricas a usar y la posibilidad de establecer el nivel de madurez de cada uno de estos procesos, pudiendo realizar una evaluación más eficiente de los mismos.

En la versión de COBIT® 5, se encuentra un nuevo componente COBIT® 5 for Information Security, presenta un modelo para la seguridad de la información enfocado en el negocio, basado en el BMIS (Business Model for Information Security).

ISACA define seguridad de la información como algo que:

Asegura que dentro de la empresa la información está protegida frente a usuarios no autorizados (confidencialidad), modificación incorrecta (integridad) y el no acceso cuando sea necesario (disponibilidad).
Dentro de las principales ventajas de este modelo encontramos:

- Entrega un modelo integral y enfocado en el negocio.
- Explica en forma detallada el modelo de negocio para gestionar la seguridad de la información.
- Se alinea fácilmente con otras normas y marcos de referencia

Este framework de COBIT® abarca principalmente:

- Información sobre los principales beneficios de la seguridad de la información para la organización.
- Aplicación de los principios de COBIT 5 por parte de los profesionales de la seguridad de la información.
- Mecanismos e instrumentos para respaldar el gobierno y la gestión de la seguridad de la información en la organización.

"*COBIT 5 for Information Security* examina las estructuras organizacionales desde una perspectiva de seguridad de la información. Define los roles y estructuras de seguridad de la información y también examina la rendición de cuentas de seguridad de la información, proporcionando ejemplos de estructuras y roles específicos y considera también las rutas potenciales de reporte de seguridad de la información y las ventajas y desventajas de cada posibilidad." [3]

V. ITIL

ITIL es un marco de trabajo orientado a la gestión de servicios, cubriendo principalmente el soporte del servicio y la prestación del servicio, el primero se encarga de garantizar la disponibilidad, continuidad y calidad del servicio prestado al usuario, mientras el segundo se enfoca en el servicio en sí mismo, en los niveles de servicio, la capacidad requerida a nivel de la infraestructura de TI, la continuidad y el grado de seguridad necesario.

A partir de esta descripción establecemos cómo este enfoque en el soporte del servicio proporcionado por ITIL se relaciona con los requerimientos o actividades de un Sistema de Gestión de Seguridad de la Información, primero porque se encarga de garantizar la disponibilidad de los servicios TI encajando con uno de los pilares de la seguridad de la información, la disponibilidad y apuntando directamente al Plan de Recuperación de Desastres y al Plan de Continuidad del Negocio buscando la continuidad de los servicios de TI, adicionalmente al entregar servicios con calidad

[3]Tomado de la presentación fundamentos de COBIT, Carlos Villamizar R.

garantiza el cumplimiento de los requerimientos del cliente, los legales y cualquier otro que sea necesario.
El proceso de la prestación del servicio contiene actividades muy importantes para el Sistema de Gestión de Seguridad de la Información, ya que nos entrega datos como los niveles de servicio, es decir que acuerdos a nivel de disponibilidad, de respuesta y solución de requerimientos o incidentes, sobre los cuales edificamos procesos como la realización y recuperación de backups, el tiempo que los servicios de TI deben estar disponibles, lo que nos permite ajustar mejor los controles implementados en el Sistema de Gestión de Seguridad de la Información, los tiempos de recuperación, y las estrategias que debemos usar para garantizar la continuidad.

La gestión de incidentes en ITIL nos da una base para la atención de incidentes con su proceso de gestión de incidentes el cual busca resolver cualquier incidente que provoque una interrupción en el servicio de la forma más rápida y eficaz. Este procedimiento ya establecido en ITIL cumple con los pasos requeridos para manejo de incidentes de Seguridad de la Información, ya que recibe el incidente, lo registra, lo clasifica y busca su resolución.

Una de los inconvenientes presentados frecuentemente en Seguridad de la Información es la gestión de cambios, labor dificultosa ya que implica el rompimiento de un paradigma en IT y es que al realizar cambios se contraen problemas, si está funcionando bien se deja como esta, es por esto común encontrar dentro de las revisiones del Sistema de Gestión de Seguridad de la Información el incumplimiento con el control de mantener actualizados los sistemas operativos, especialmente servidores, aunque no soluciona los inconvenientes técnicos que se generan de estos cambios, si entrega un procedimiento ya establecido y una serie de pasos para realizar estos cambios minimizando la posibilidad de que se presentes inconvenientes.

VI. ISO/IEC 27001 - ISO/IEC 27002

Ya vimos cómo abordar desde la parte de gestión y gobierno la implementación de un Sistema de Gestión de Seguridad de la Información, pero ¿qué debe contener dicho sistema?, para resolver esta inquietud podemos tomar como guía la norma ISO-IEC 27001 Sistema de Gestión de Seguridad de la Información y la ISO-IEC 27002 Código de práctica para Gestión de Seguridad de la Información.

La primera nos entrega los requisitos que debería tener un Sistema de Gestión de Seguridad de la Información, esta norma es certificable pero se puede hacer uso de ella como guía incluso si la empresa o entidad no desea certificarse. La segunda la ISO-IEC 27002 nos ayuda a realizar la implementación de cada uno de los requisitos expuestos en la ISO-IEC 27001.

Dentro de la ISO-IEC 27001 de requisitos para la implementación del Sistema de Gestión de Seguridad de la Información de los cuales no se pueden excluir los numerales del 4 al 10 dentro de los cuales se realizar actividades como el conocimiento de la organización, establecimiento de la política de seguridad de la información, roles, responsabilidades, valoración y tratamiento de riesgos, capacitación y toma de conciencia, auditorías, mejora continua entre otros.

Adicionalmente, nos entrega un anexo con los objetivos de control e información que nos permitirá definir nuestras políticas, procedimientos, estándares y controles a documentar e implementar

haciendo más fácil la labor de implementación del Sistema de Gestión de Seguridad de la Información. Aunque esta norma no es la única para la implementación, gestión y auditoria de Sistemas de Gestión de Seguridad de la Información.

VII. REGULACIÓN Y LEGISLACIÓN

Actualmente en Colombia existen diversas leyes que propenden por la seguridad de la información, dentro de ellas encontramos la ley 1581 de 2012 junto con su decreto reglamentario 1377 de 201, por las cuales se dictan disposiciones generales para la protección de datos personales, dicha ley aplica para cualquier base de datos de datos personales que sea suceptible de tratamiento por entidades publicas o privadas.
Por lo cual es una ley de aplicación general ya que en esta era de la información casi cualquier empresa procesa, almacena o trata de alguna manera datos personales, adicionalmente entrega uno principios para el tratamiento de esta información los cuales se deben cumplir a cabalidad, estipula los datos sensibles y como deben ser tratados y los derechos de los titulares siendo lo mas importante la autorización previa del mismo para que su información sea objeto de tratamiento.

La ley 1273 de 2009 que modifico el codigo penal y creo un bien juridico denominado “de la protección de la información de los datos”, estableciendo legalmente que acciones atentan contra la confidencialidad, integridad y disponibilidad de los datos y los sistemas de información.

Es claro la aplicabilidad de estas normas para cualquier entidad publica y privada, entre otras dependiendo del sector en que se desarrolle su actividad económica, como lo es la circular 042 de 2012 para el sector financiero, a fin de no incurrir en contravenciones contra las mismas al implementar el Sistema de Gestión de Seguridad de la Información y los controles respectivos.

VIII. INTEGRACIÓN

En este artículo he mencionado solo algunos de los modelos, marcos de trabajo, y regulaciones vigentes relacionados con la seguridad de la información, existen bastantes los cuales se pueden usar por separado, integrándolos, implementándolos total o parcialmente, dependiendo del alcance que le quiera dar la empresa, de la manera en que gestiona sus procesos, la capacidad de entregar los recursos necesarios, teniendo en cuenta hasta la cultura, costumbres, ubicación geográfica entre otros, lo único que debe cumplir a cabalidad son los requerimientos regulatorios y legales.

Se convierte en un desafío saber con qué marco o estándar trabajar, si usar uno, varios o todos, por lo que es necesario conocer muy bien la empresa, para saber cuál se adapta mejor, no se debe sobrecargar los procedimientos y a las personas al implementar los modelos, se debe establecer correctamente los recursos requeridos, en cuanto a costos, conocimientos, tiempos y características que puedan afectar su adopción.

IX. CONCLUSIONES

La falta de conocimiento en gestión de Seguridad de la Información puede llevar a tratar de realizarla de una manera heroica al comenzar de cero o de una manera catastrófica al implementar normas o marcos de trabajo incorrectos.

La buena gestión de un Sistema de Seguridad de la Información desde su planeación, pasando por todas las etapas de vida del mismo, conlleva a obtener una implementación exitosa, una gestión simple, y

una integración efectiva a los procesos de la empresa.

Todos los modelos o marcos de trabajo requieren de un compromiso constante, de seguimiento, medición, y del conocimiento del componente humano ya que ninguno se desarrolla por sí solo.

X. REFERENCIAS

[1] PROJECT MANAGMENT INSTITUTE "Guía del PMBOK® "Quinta edición. 2013.
[2] GOVERNANCE INSTITUTE "COBIT 4.1". 2007.
[3] ISACA "COBIT® 5". 2012.
[4] KNOWLEDGE & PRACTICE "Preparación para el examen de certificación PMP®" Sandra M. Mercado - Ene. 2013
[5] ICONTEC® "NTC-ISO-IEC 27001" – Dic. 2013
[6] SEGURINFO XIX Congreso y Feria Interamericana de Seguridad de la Información "RE-EVOLUCION COBIT® 5" Patricia Prandini, Rodolfo Szuster - Marzo 2012
[7] RISK MEXICO " Desarrollo de una cultura de Gestión de Continuidad del Negocio en América Latina" Jorge Escalera – Abril 2012
[8] CONGRESO DE COLOMBIA "Ley Estatutaria 1581 de 2012" Octubre de 2012
[9] CONGRESO DE COLOMBIA "Ley 1273 de 2009" Enero de 2009
[10] SUPERINTENDENCIA FINANCIERA DE COLOMBIA "Circular Externa 042" Octubre de 2012

Autor

Juan de Jesús Aponte Buitrago
Ing. de Sistemas
Estudiante Especialización en Seguridad Informática
Universidad Piloto de Colombia