GESTIÓN DE LA SEGURIDAD Y EL RIESGO EN TI

Romero Ussa, Katherine Astrid.
Katherine.romerou@gmail.com
Universidad Piloto de Colombia

Resumen— Este documento busca contextualizar al lector en cómo gestionar la seguridad y el riesgo en un ambiente de TI, utilizando los modelos más conocidos del mercado en este momento, brindándole opciones desde como abarcar el tema de seguridad en TI, como reconocer los riesgos y actuar frente a ellos hasta que controles implementar según el caso para mitigar los mismos y brindar seguridad a la compañía.

Abstract— This document looks for to contextualize to the reader in how managing the security and the risk in an atmosphere of TI, using the models more known the market at this moment, offering options him from like including the subject of security in TI, like recognizing the risks and of acting them in front of until controls to implement according to the case to mitigate such and to offer security to the company.

Índice de Términos— Seguridad, Riesgo, Seguridad Informática, Seguridad de la Información, Gobierno de TI, Gobierno de Seguridad de la Información, ISO 27002, COBIT, ISO 27005, ISO 31000.

I. INTRODUCCIÓN

Gestión de la seguridad y el riesgo en TI, un título amplio, que nos deja pensar en muchos posibles contenidos para él, muchas personas que lean este artículo pueden llevarse una idea global de lo que tratara, sin embargo es conveniente que se canalice la finalidad del mismo. Si bien cuando nombramos seguridad y riesgo lo primero que imaginamos es que vamos a proteger un algo para tratar de mitigar un riesgo existente sobre él, en general esto es lo que veremos reflejado en este artículo, pero más que la relación de seguridad y riesgo lo que se busca con este, es darle una idea al lector de cómo realizar la gestión de estos factores en un ambiente de TI, no es lo mismo hablar de un riesgo económico por la subida del dólar, que hablar de un riesgo de que la plataforma de clientes se caiga en el momento de mayor operación de la compañía, esto para ambientar un poco el tema, en fin en este documento encontrara como manejar seguridad y riesgo tanto por separado como en conjunto utilizando las herramientas de gestión más conocidas en la actualidad (ISO27001, COBIT, entre otros).

II. GESTIÓN DE LA SEGURIDAD Y EL RIESGO EN TI

En los últimos años hemos visto el crecimiento tecnológico en todos los ámbitos conocidos, así como cada día encontramos nuevas herramientas sofisticadas y con mas funcionalidades por la evolución tecnológica, también encontramos que ese avance se está implementando para contravenir la seguridad de la información en cualquier ámbito con el fin de causar un daño al ente atacado, por lo anterior es de vital importancia concienciarnos de que poseemos un riesgo inminente de ser atacados en cualquier momento y por lo cual debemos prepararnos para contrarrestar el mismo.

Enfocándonos más en el tema especifico de este artículo, teniendo en cuenta lo mencionado anteriormente, perteneciendo a un área de TI, el riesgo es mucho mayor, por la infraestructura manejada, por los tipos de accesos que se poseen y por la información a la que podemos llegar a acceder bien sea de manera intencionada o no, adicional a esto debemos ser consientes de que en la mayoría de estas áreas no hay una conciencia real del riesgo que se corre y por lo mismo no hay conciencia de la generación de un plan de seguridad con el fin de mitigar la ocurrencia del mismo, es por esto que a través de este artículo se presenta la estrategia que se sugiere implementar para

implementar seguridad en las áreas de TI.

Como primera instancia es importante que se implemente un gobierno de TI (en los casos en que no exista) cuya finalidad será agregar valor a través su gestión que debe está alineada con los objetivos del negocio la cual permita mitigar los riesgos y así generar un retorno sobre la inversión (quizá no monetario) a través de beneficios para la empresa, el gobierno de TI se conforma de las siguientes áreas de enfoqué [i]:

- Alineamiento estratégico
- Entrega de valor
- Administración de riesgos
- Administración de recursos
- Medición del desempeño

Nos enfocaremos en el área de administración del riesgo mediante la cual observaremos que su buen manejo ayudara con el cumplimiento de los objetivos de las demás, esta área requiere:

- Conciencia de riesgo por parte de los altos directivos de la compañía.
- Entendimiento claro del apetito de riesgo de la empresa.
- Entendimiento de los requerimientos de cumplimiento.
- Transparencia sobre los riesgos significativos de la empresa.
- Implementar las responsabilidades de la administración de riesgos dentro de la compañía.

Los enunciados anteriores no solo son aplicables al área de administración de riesgos en TI, estos son aplicables a cualquier área de administración de riesgos de cualquier gobierno, como por ejemplo el gobierno de seguridad de la información cuya implementación es igual de indispensable que el gobierno de TI y con quienes debemos trabajar de la mano para que surjan y se lleven a cabalidad los objetivos de TI en cuanto a seguridad y gestión del riesgo.

Enfocándonos un poco más hacia el gobierno de seguridad de la información una de sus principales funciones es generar políticas de seguridad en los diferentes campos que administran una de ella sin duda debe ser la *política de seguridad informática*, la cual debe ser estructurada en compañía del gobierno de TI y en la cual debe estar plasmado el plan de seguridad sobre la estructura tecnológica de la compañía; pero para llegar a este punto primero debemos tener claridad sobre que poseemos, que es lo más crítico, y sobre todo que es lo que queremos proteger (de valor para la compañía), una vez definido esto es importante realizar un análisis de riesgos sobre los mismos y con base en él, establecer la política, una vez establecida debemos definir cómo vamos a hacerla cumplir, para ello debemos implementar controles. En resumidas cuentas ya hemos entregado el paso a paso de cómo gestionar el riesgo, pero esto ha sido muy general, ahora veremos esta misma estructura mucho más desglosada y con la sugerencia de uso de cada uno de los modelos relacionados.

III. COBIT

Es un modelo de referencia para implementar gobierno de TI en las compañías, en mi concepto COBIT es el modelo perfecto para definir *qué hacer*, en este se proponen 5 principios básicos con los cuales alinea toda su estructura, estos son [ii]:

- Satisfacer las necesidades de las partes Interesadas
- Cubrir la compañía de forma integral
- Aplicar un solo marco integrado
- Habilitar un enfoque holístico
- Separar el gobierno de la administración

De estos cinco principios, los dos primeros principios "*satisfacer las necesidades de las partes interesadas"* y "c*ubrir la compañía de forma integral"* son en los que se contempla una de las bases importantes que estamos tratando y es la gestión de riesgos.

Como lo mencione antes en este documento COBIT es un excelente marco para indicarnos que hacer para implementar un buen gobierno de TI y estructurar su organigrama de manera adecuada estableciendo las funciones necesarias e impartiéndolas a las áreas que deban realizarlas,

pero también viene el cómo, si bien se puede tener una buena estructura pero no contamos con los procesos indicados, la correcta gobernabilidad se va a ver afectada ya que no está arrojando los resultados esperados, es por esto que a nivel del como la ISO 27002 es la mejor opción para indicar como realizar las tareas en pro de la seguridad de la información en un ambiente de TI y la ISO 27005 es la mejor opción para indicar como realizar las tareas en pro de gestionar los riesgos en seguridad de la información en un ambiente de TI, por lo cual a continuación les presento los dos modelos, su estructura.

IV. ISO 27002

Es un estándar para la seguridad de la información, el cual sirve como guía de mejores prácticas a implementar con el fin de mitigar los riesgos en seguridad de la información, este modelo está conformado de los siguientes dominios [iii]:

- Organización de la seguridad de la información.
- Seguridad de los recursos humanos.
- Gestión de los activos.
- Control de accesos.
- Criptografía.
- Seguridad física y ambiental.
- Seguridad de las operaciones:
    - Procedimientos y responsabilidades
    - Protección contra malware
    - Resguardo
    - Registro de actividad y monitorización
    - Control del software operativo
    - Gestión de las vulnerabilidades técnicas
    - Coordinación de la auditoría de sistemas de información.
- Seguridad de las comunicaciones:
    - Gestión de la seguridad de la red
    - Gestión de las transferencias de información.
- Adquisición de sistemas, desarrollo y mantenimiento:
    - Requisitos de seguridad de los sistemas de información
    - Seguridad en los procesos de desarrollo y soporte
    - Datos para pruebas.
- Relaciones con los proveedores:
    - Seguridad de la información en las relaciones con los proveedores
    - Gestión de la entrega de servicios por proveedores.
- Gestión de incidencias que afectan a la seguridad de la información:
    - Gestión de las incidencias que afectan a la seguridad de la información
    - Mejoras.
- Aspectos de seguridad de la información para la gestión de la continuidad del negocio:
    - Continuidad de la seguridad de la información
    - Redundancias.
- Conformidad:
    - Conformidad con requisitos legales y contractuales
    - Revisiones de la seguridad de la información.

Como observamos es un estándar muy completo con el cual podemos hacer gestión total sobre la seguridad de la información en cualquier ambiente de TI, en este artículo no vamos a entrar a profundizar sobre cada uno de los puntos ya que se extendería demasiado y podríamos perder el hilo de la razón del mismo, para argumentar un poco más sobre el cómo, este modelo trae en sus anexos los controles que se deben implementar en cada uno de los puntos, los cuales son muy completos ya que

contemplan el abarcamiento de la mayoría de posibles escenarios existentes.

V. ISO 27005

Es un estándar para la gestión de riesgos en seguridad de la información, el cual sirve como guía de la implementación que se debe realizar para tratar los riesgos en seguridad de la información, este modelo está conformado de los siguientes puntos sobresalientes [iv]:

- Evaluación de riesgos de seguridad de la información (ISRA)
- Tratamiento de riesgos de seguridad de la Información
- Información de admisión de riesgos de seguridad
- Información de comunicación de riesgos de seguridad
- Información seguimiento de riesgos de seguridad y revisión

Cada uno de los ítems anteriores debe ser implementado en cada uno de los dominios propuestos por la ISO 27002, esto permitirá que la gestión del riesgo sea completa en el ambiente de TI, el cómo realizarlo se puede encontrar en los anexos del modelo.

VI. ISO 31000

Bueno mucho se ha dicho sobre buenas prácticas, controles, seguimiento de modelos, pero en si la esencia de la seguridad de la información se encuentra en realidad en hacer una buena gestión de los riesgos es por esto que me atrevo a comentar un poco en este artículo sobre la ISO 31000 que es un estándar global de gestión de riesgos (no solo de seguridad de la información) que nos permite conocer a profundidad como realizar una buena gestión de riesgos, los puntos que propone son los siguientes [v]:

- Diseño de marco para la gestión de riesgos
    - Comprensión de la organización y su contexto
    - Establecimiento de políticas de gestión de riesgos
    - Rendición de cuentas
    - La integración en los procesos de organización
    - Recursos
    - Establecimiento de la comunicación interna y mecanismos de informes
    - Establecimiento de la comunicación externa y mecanismos de informes
- La implementación de la gestión de riesgos
    - Aplicación del marco para la gestión del riesgo
    - Implementación del proceso de gestión de riesgos
- Seguimiento y revisión del marco
- Mejora continua del marco
- Establecimiento del contexto
    - Generalidades
    - Establecimiento del contexto externo
    - Establecer el contexto interno
    - Establecer el contexto del proceso de gestión de riesgos
    - Definición de los criterios de riesgo
- Evaluación del Riesgo
    - Generalidades
    - Identificación del riesgo
    - Análisis de riesgo
    - Evaluación de riesgos
- Tratamiento del riesgo
    - General
    - Selección de las opciones de tratamiento de riesgos
    - Preparación y ejecución de planes de tratamiento de riesgo
- Seguimiento y revisión
- Registro del proceso de gestión de riesgos

El marco anterior es solo para que nos hagamos

una idea del trabajo que se debe desarrollar con los riesgos, si bien esta estructura puede parecer compleja, no lo es cuando se tiene un buen conocimiento sobre el tema, definitivamente esta no es nuestra especialidad pero lo importante es que si en la organización no se cuenta con un área de riesgos, seamos capaces de reconocerlos y tratarlos, para ello les comparto las siguientes herramientas que pueden servir para el tratamiento de los riesgos[vi].

1. Conocer el significado de los siguientes conceptos:

   - Activo: Un activo es algo que tiene valor para la organización por lo tanto requiere protección.
   - Vulnerabilidad: Debilidad inherente al activo. Su presencia no causa daño por sí misma, ya que necesita que se presente una amenaza que la explote.
   - Amenaza: Una circunstancia o evento que tiene el potencial de causar daño a un activo por lo tanto a la organización.
   - Impacto: Daño causado por una amenaza que explota una vulnerabilidad de un activo y que afecta adversamente el logro de los objetivos del negocio.
   - Riesgo de seguridad de la información: El potencial de que una cierta amenaza explote vulnerabilidades de un activo o grupo de activos y así cause daño a la organización.

2. Como medir un riesgo:

   - Posibilidad / probabilidad de que ocurra un evento
   - Sus Consecuencias / impacto

3. Gestionar efectivamente los riesgos a través de:

   - Entendimiento de las amenazas, las vulnerabilidades y el perfil de riesgo del área de TI en base al de la organización.
   - Entendimiento de la exposición al riesgo y las posibles consecuencias de la inestabilidad.
   - Conciencia de las prioridades de la gestión de riesgos con base en las posibles consecuencias
   - Estrategia organizacional de mitigación de riesgos adecuada para obtener consecuencias aceptables
   - Aceptación / atención organizacional con base en un entendimiento de las posibles consecuencias del riesgo residual
   - Evidencia cuantificable de que los recursos de la gerencia se utilizan de forma apropiada y con adecuada relación de costo / beneficio

4. Roles y responsabilidades (en las compañías donde pueda ser aplicada o en su defecto su posible representación a pequeña escala):

   - Consejo de dirección y alta dirección: Garantizar que los recursos necesarios se apliquen efectivamente para desarrollar las capacidades necesarias para el logro de la misión
   - Director de informática: Responsable de la planificación, el presupuesto y el rendimiento de TI, incluyendo los componentes de TI.
   - Gerente de seguridad de la información: Son los responsables de los programas de seguridad de la información en las organizaciones, generalmente incluyen la gestión de riesgos.
   - Propietarios de sistemas de información: Son los responsables de que existan los controles de seguridad apropiados para preservar la confidencialidad, integridad y disponibilidad de la información y los sistemas de TI
   - Gerentes de unidades de negocio: Son responsables de las operaciones de negocio y los procesos de adquisiciones de TI, deben asumir roles activos en el programa de gestión de riesgos
   - Profesionales de seguridad IT: Son responsables de la implementación apropiada de los requerimientos de seguridad

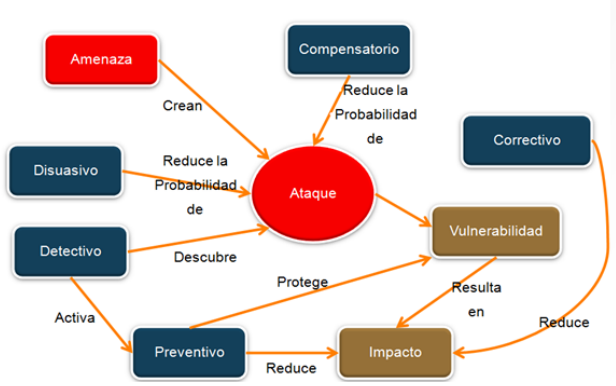
5. Actividades de la gestión de riesgos:

   - Identificación de riesgos

- Estimación de riesgos
- Evaluación de riesgos
    - Criterios de aceptación de riesgos
    - Criterios para realizar evaluaciones de riesgos
    - Identificar los riesgos de la seguridad de la información
    - Identificar los dueños de los riesgos
    - Analizar los riesgos de la seguridad de la información
    - Evaluar las consecuencias
    - Evaluar la probabilidad
    - Determinar los niveles de riesgo
- Tratamiento de riesgos
    - Seleccionar las opciones apropiadas de tratamiento de riesgos
    - Determinar los controles que sean necesarios
    - Comparar los controles que sean necesarios
    - Comparar los controles determinados
- Aceptación de riesgos

6. Factores presentes en la identificación de riesgos:

- Activos
- Amenazas
- Controles
    - Preventivo
    - Detectivo
    - Disuasivo
    - Correctivo
    - Compensatorio



1. *Control del Riesgo. Imagen tomada de material de apoyo Gestión de Riesgo de Seguridad GSI ESI Universidad Piloto de Colombia*

La imagen anterior nos muestra la relación entre los actores que participan en un eventual riesgo con la implementación de los posibles controles que pudieran mitigarlo.

- Vulnerabilidades
- Impactos y consecuencias

2. Factores de tratamiento de riesgos

- Reducir o mitigar
- Asumir o retener
- Evitar
- Transferir

2. *Tratamiento del Riesgo. Imagen tomada de material de apoyo Gestión de Riesgo de Seguridad GSI ESI Universidad Piloto de Colombia*

La imagen anterior nos muestra todos los actores que se encuentran inmersos en la gestión de riesgos (mencionados en detalle en un apartado anterior) y

la relación entre ellos.

Básicamente en la información anterior se resume la gestión de riesgos de cualquier tipo, si utilizamos estas herramientas para definir los riesgos en TI lograremos un excelente tratamiento para los mismos, lo importante es conocer nuestra infraestructura, que información manejamos, cuales activos son fundamentales para la organización, que amenazas pueden afectar esos activos, si tenemos vulnerabilidades presentes, que podemos hacer para minimizar el riesgo de que se explote esa vulnerabilidad y que tratamiento realizaremos si se llega a desarrollar un riesgo.

VII. CONCLUSIONES

- Para implementar gestión de seguridad y el riesgo en seguridad de la información en un ambiente de TI es importante valerse de la siguiente estructura:
    - Implementar un gobierno de TI
    - Implementar un gobierno de seguridad de la información
    - Seguir la estructura de gobernabilidad de los modelos propuestos en el artículo en los cuales se establece que debemos estar alineados con los objetivos estratégicos de la organización
    - Conociendo lo anterior, seguir el modelo de gestión de riesgos para identificarlos y realizar las tareas de mitigación respectivas
    - Mitigando la ocurrencia de los riesgos brindamos seguridad a los activos de la compañía
    - Debemos jerarquizar los activos para identificar cuáles son los más críticos y gestionarlos de manera inmediata (sin dejar a un lado los demás)

- COBIT es un modelo que podemos utilizar en COMO implementar gobierno de seguridad de la información y de TI

- ISO 27002 es un modelo de buenas prácticas de seguridad, que podemos utilizar en el QUE hacer para cumplir con los objetivos de la implementación del Gobierno de TI a través de los dominios propuestos en el mismo.

- ISO 27005 es un modelo de gestión de riesgos en seguridad de la información que podemos utilizar para la mitigación de los mismos existentes en ambientes de TI.

- ISO 31000 es un modelo de gestión de riesgos en general, muy completo del cual podemos tomar varias herramientas para la gestión de riesgos de seguridad de la información presentes en un área de TI

REFERENCIAS

[i] CISM Certified Information Security Manager – Capitulo 1 - Gobierno de Seguridad de la Información

[ii] Introducción a COBIT 5 – Los 5 principios de COBIT
http://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt

[iii] ISO 27002 Guía de Buenas Prácticas en Seguridad de la Información
http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39612

[iv] Contenido ISO 27005
http://www.27000.org/iso-27005.htm

[v] ISO 31000 Risk management — Principles and Guidelines

[vi] Material de apoyo Gestión de Riesgo de Seguridad GSI ESI Universidad Piloto de Colombia

Autor

Realizado por:
Katherine Astrid Romero Ussa
Ingeniera de Sistemas

Especialista en Seguridad Informática (En Proceso)
Gestión de la Seguridad y el Riesgo en TI
Universidad Piloto de Colombia
2015

"En este documento se expone una propuesta de implementación de gestión de la seguridad y el riesgo en un ambiente de TI, utilizando los modelos más conocidos del mercado como lo son COBIT y la familia ISO 27000; en ningún momento infiere que sea una verdad absoluta ni un paso a seguir estricto para llegar a tal fin, el lector esta en decisión de tomar o abolir las recomendaciones presentadas en este artículo".