Metodología y gobierno de la gestión de riesgos de tecnologías de la información

Methodology and Governance of the IT Risk Management

Ricardo Gómez[a], Diego Hernán Pérez[b], Yezid Donoso[c], Andrea Herrera[d]

PALABRAS CLAVES

Amenazas en TI, análisis de riesgos, continuidad de negocios, gobernabilidad de TI, Vulnerabilidad.

KEY WORDS

Business continuity, IT governance, risk analysis, vulnerability and threat in IT.

RESUMEN

Las organizaciones cada vez son más conscientes de los impactos que les pueden generar los riesgos referentes a las Tecnologías de Información (TI). Es frecuente que empresas de diversos sectores económicos reporten pérdidas debido a fallas y/o ataques sobre sus servicios de TI, los cuales afectan seriamente su reputación y su solidez financiera y operacional. Existen dos pilares fundamentales para realizar el análisis de riesgos: los estándares y normas, de un lado, y las metodologías, de otro; estos pilares por sí solos no aseguran el éxito si no se articulan adecuadamente. En este artículo mostramos qué tipo de estándares y normas se deben considerar al realizar un análisis de riesgos, posteriormente explicamos cómo utilizar una metodología y cómo articularla en el proceso de gobernabilidad de TI para desarrollar en forma exitosa este tipo de iniciativas.

ABSTRACT

The organizations are more interested in the impact that can generate risk and in particular associated to IT. Every day it is possible to see that different business of sectors like: finance, governance, health, production, among others, they are reporting economical lost due to fails or attacks over theirs IT services, which can affect the reputation, relationships with the clients and their self financial and operational robustness. There are two fundamental pillars for the risk analysis: standards and norms and the other side the methodologies; with these pillars along is impossible to assure the results without the governability of this risk analysis. In this paper, we show what kind of standards and legal documents must be considered in a risk assessment process and after we are going to explain how is possible to use a methodology and how to connect this methodology with the IT governance process in a successful way.

a Ingeniero de Sistemas y Computación. Ingeniero de Proyectos CIFI – Informática. Facultad de Ingeniería. Universidad de los Andes. Bogotá D.C., Colombia.
✉ricgomez@uniandes.edu.co

b Ingeniero industrial, Especialista en sistemas de información. Consultor en temas de estrategia y procesos de TI. Profesor catedrático. Facultad de Ingeniería. Universidad de los Andes. Bogotá D.C., Colombia.
✉perezdiegohernan@yahoo.com

c Ph.D. en Tecnologías de Información. Profesor Asociado, Departamento de Ingeniería de Sistemas y Computación. Grupo COMIT. Facultad de Ingeniería. Universidad de los Andes. Bogotá D.C., Colombia.
✉ydonoso@uniandes.edu.co

d M.Sc. Magíster en Ingeniería de Sistemas y Computación. Instructora, Departamento de Ingeniería de Sistemas y Computación. Grupo TION. Facultad de Ingeniería. Universidad de los Andes. Bogotá D.C., Colombia.
✉a-herrer@uniandes.edu.co

INTRODUCCIÓN

Las organizaciones son cada vez más conscientes de lo que significan los riesgos informáticos y, sobre todo, han aprendido que en la mayoría de los casos deberán coexistir con ellos pero en forma controlada. Debido a tantos efectos negativos que se han visto en las organizaciones por las amenazas sobre los servicios de TI, aquéllas han comenzado a exigir, dentro de sus funciones normales internas, un análisis de riesgo y un plan de mitigación; así mismo, han entendido que siempre quedará un riesgo remanente y latente en sus procesos de misión crítica. También es importante mencionar que nuestras ciudades cada vez hacen mayor uso de las tecnologías de la información para ser más eficaces y efectivas, con el fin de lograr el cumplimiento de su desarrollo y de sus políticas de seguridad; es por esta razón que el análisis y entendimiento de los riesgos de TI involucran directamente a las ciudades; además, los riesgos de TI forman parte de los riesgos que cualquier dirigente debe tener en cuenta en su gobierno.

Es conocido por todos que el tratamiento del riesgo puede estar enfocado de cuatro formas tradicionalmente: establecer controles para mitigarlos, aceptar el riesgo tal y como está porque es imposible establecer controles, eliminar el riesgo quitando los procesos del negocio que los generan y, finalmente, trasladar el riesgo a un tercero; por ejemplo, a través de seguros. Establecer controles significa la generación de políticas, normas y procedimientos que conlleven a la mitigación del riesgo; por supuesto, en el caso de TI, generalmente conlleva al final a la configuración de estas políticas en diferentes procedimientos, equipos de hardware, aplicaciones, sistemas operativos, entre otros. Por su parte, aceptar el riesgo significa que la empresa asume y conoce perfectamente cuál sería el impacto en el negocio si este riesgo se materializa. Por otro lado, en la mayoría de los casos, eliminar los procesos que conllevan al riesgo significaría cambiar el quehacer (negocio) de la organización y, por supuesto, tradicionalmente la organización no permitirá que esto suceda. Por último, está el traslado del riesgo a través de pólizas, figura muy utilizada por las compañías; en este caso, es necesario tener muy claro cuál sería la probabilidad de que este riesgo se lleve a cabo, para realizar un balance entre el costo y el beneficio de tener ese seguro. Respecto a esta estrategia hay que ser consciente de que está muy relacionada con el cubrimiento económico de la materialización de un riesgo, porque quien deberá asumir el impacto en términos de imagen y de relación con sus interesados será la organización.

Para tomar la decisión sobre qué tipo de estrategia utilizar, se hace necesario realizar un análisis de cada riesgo para conocer y cuantificar el impacto de que el riesgo se lleve a cabo, así como su probabilidad de ocurrencia. Ahora, estas decisiones de qué hacer con los riesgos deben estar alineadas con el esquema estratégico de la organización; esto significa que el gobierno de TI es una pieza clave dentro de este proceso, para asegurar la pertinencia y el éxito de las decisiones que se tomen respecto a los riesgos.

Observando las necesidades que las organizaciones tienen hoy en día en cuanto a los riesgos de TI, es que hemos decidido presentar este artículo, el cual se ha enfocado primero en mostrar un marco de referencia en cuanto a estándares, normas, reglamentaciones, entre otros, relevantes al análisis de riesgos. Como segundo enfoque mostramos una metodología comprobada con casos de éxitos a nivel internacional, sobre cómo llevar a cabo un análisis de riesgos. Finalizamos nuestro artículo mostrando los aspectos más relevantes del gobierno de TI respecto a la gestión de los riesgos.

ORÍGENES DE LA REGULACIÓN Y SU PAPEL EN LA FORMALIZACIÓN DE LA GESTIÓN DE RIESGOS DE TI

El riesgo ha existido inherente a cada acción que realiza el ser humano. Sin embargo, en la sociedad actual, inmersa en un ambiente altamente tecnológico y donde la información es el centro de las actividades, se ha desarrollando una creciente dependencia de las TI lo que las ha convertido en un gran factor de riesgo

y quizás, uno de los más importantes de este siglo. Por supuesto, las empresas no han sido ajenas a este proceso porque, al apoyarse en TI para mejorar su eficiencia y productividad, entregan a éstas una buena porción de responsabilidades críticas para el negocio. Pero, como es bien sabido, no existe tecnología perfecta; todas presentan deficiencias, vulnerabilidades, errores, entre otros. Además, si los procesos de negocio dependen de TI, el riesgo incrementa y más aún si esta tecnología es utilizada por personas en el desarrollo de dichos procesos. Lo anterior genera lo que se conoce como riesgo de TI; es necesario gestionar estos riesgos porque no hacerlo puede generar altos costos para la organización [1].

Algunas empresas han vivido experiencias realmente complejas que han demostrado la necesidad de hacer dicha gestión: el caso de Comair, una empresa subsidiaria de Delta Air Lines, resalta algunas consecuencias de la materialización del riesgo de TI. En diciembre de 2004, Comair experimentó un incidente con su sistema de planeación de horarios para tripulaciones [2]. Este sistema, de misión crítica para la operación del negocio, dejó de funcionar el 24 de diciembre y causó una interrupción total de sus vuelos, dejando pérdidas equivalentes a las utilidades operativas de todo un trimestre. Otro caso es el de "CardSystems Solutions Inc.", procesadora de tarjetas de crédito. A mediados del 2005 reportó que individuos desconocidos obtuvieron acceso a las transacciones de 40 millones de tarjetahabientes. Visa y Mastercard, clientes de CardSystems, cancelaron su negocio con la empresa, que luego fue vendida [2]. Un caso colombiano muy reciente, dado a finales de febrero de 2010, fue el que afectó a los clientes de un banco reconocido, quienes tras una falla originada por la saturación de una de las aplicaciones visualizaron inconsistencias en la actualización de sus saldos; afortunadamente, en ningún momento se afectaron realmente los saldos de las cuentas, sin embargo, la institución financiera tuvo que activar sus contingencias para minimizar el impacto de la falla tecnológica [3]. Finalmente, se puede presentar el caso del LHC[1] de CERN. Este acelerador de partículas, catalogado como el más grande del mundo, intenta recrear condiciones similares a las del "Big-Bang" mediante altas energías; por lo tanto, sus experimentos deben ser minuciosamente controlados. Sin embargo, el 10 de septiembre de 2008 un grupo de hackers ingresó a uno de los sistemas del LHC y modificó su sitio web. Favorablemente, el ataque no tuvo intenciones maliciosas y colaboró con identificar vulnerabilidades del sistema. La intrusión, de haber sido mal intencionada, no sólo pudo haber causado daños en los modernos instrumentos del laboratorio sino que también pudo haber causando una catástrofe. ¡Ojalá todos los negocios tuvieran la suerte de CERN! No obstante, éste es un caso muy poco común y la materialización de los riesgos de TI suelen terminar en un desastroso "Big-Bang" [4].

Estas organizaciones tuvieron algo en común: la inapropiada gestión de riesgos de TI. Su efecto, no obstante se extendió desde TI hasta afectar directamente la operación y la misión del negocio: se manifestó el riesgo de TI como riesgo corporativo, haciendo que su interés sea igualmente corporativo y no un problema limitado estrictamente al área de TI. Pero, la creciente dependencia en las TI no es sólo un riesgo para los negocios, también se está convirtiendo en una amenaza para países enteros. El caso de India, un país que ha desarrollado de manera notable su industria del software, se encuentra en el dilema de la dependencia en soluciones TI. Este país ha implementado innumerables soluciones de TI para apoyar activos gubernamentales como (plantas nucleares, servicios públicos domiciliarios, grandes centros de manufactura y propiedades públicas y privadas, entre otros) lo cual conlleva a que exista un alto riesgo de ataques terroristas a través de vulnerabilidades de los sistemas de TI correspondientes. Tan es así, que el gobierno y muchas empresas indias se encuentran en constantes discusiones para tomar medidas preventivas [5]. Este riesgo no

1 Large Hadron Collider (LHC) es el acelerador de partículas más grande del mundo, ubicado en Conseil Européen pour la Recherche Nucléaire (CERN).

será un problema sólo de la India; muchos otros países entrarán, en mayor o menor medida, en los niveles de implementación de soluciones de TI de los países más desarrollados, por tanto, se presentará de igual manera este grave riesgo para la seguridad nacional.

Debido a lo mencionado anteriormente, los gobiernos han establecido estrictas reglamentaciones y regulaciones que buscan minimizar los riesgos operativos, muchos de éstos asociados con las TI de las compañías. Se han creado mecanismos que permiten regular la actividad, fijar los criterios técnicos y jurídicos que faciliten el cumplimiento de dichas leyes, normas y circulares. Ejemplos de estas regulaciones son abundantes y especificas por sector y no se pretende ahondar en ellas; no obstante, queda claro que adicionalmente a los beneficios que puede traer una adecuada gestión de los riesgos de TI para una compañía, nace la necesidad del cumplimiento.

A raíz de lo anterior, surge la necesidad de crear estándares para el análisis y gestión de riesgos; éstos se conocen comúnmente como *Frameworks* o Marcos de Trabajo [6]. Entre los marcos de gestión de riesgos de TI más conocidos se encuentran los siguientes: NIST [7], IT Risk [2], Risk IT [8], Octave [9], Magerit [10], entre otros. El objetivo de estos marcos es el de integrar buenas prácticas mundialmente reconocidas de forma ordenada y sistemática. Estos marcos están diseñados para facilitar el análisis de riesgos y orientan en la implantación de un sistema de gestión de riesgos.

UNA METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS DE TI

El hecho de conocer los marcos de referencias para el análisis de riesgo no asegura que el proceso se lleve a cabo en forma exitosa. Es por esto que se requiere adicionalmente de una metodología que, en forma eficaz y eficiente, aplique los marcos de referencias exitosamente en la labor del análisis de riesgos de TI. Lo anterior conlleva a que se identifiquen y prioricen exhaustivamente los diferentes riesgos para definir planes de acción y de protección, acordes con cada uno. La labor en general no es una tarea fácil, ya que involucra un estudio detallado de todas las áreas de la organización y un análisis crítico que garantice la adecuada identificación y priorización de los riesgos y vulnerabilidades. Se hace necesario, entonces, contar con metodologías que faciliten el logro de estos objetivos de altos volúmenes de información.

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) [9] es una metodología desarrollada por el CERT/CC[2] [11, 12] que tiene por objeto facilitar la evaluación de riesgos en una organización. En esta parte del artículo, presentaremos una visión general de OCTAVE y mostraremos de manera global el modo cómo se desarrolla.

PRINCIPALES CARACTERÍSTICAS

OCTAVE se centra en el estudio de riesgos organizacionales [13] y se focaliza principalmente en los aspectos relacionados con el día a día de las empresas. La evaluación inicia a partir de la identificación de los activos relacionados con la información, definiendo este concepto como los elementos de TI que representan valor para la empresa (sistemas de información, software, archivos físicos o magnéticos, personas, entre otros). De esta forma, OCTAVE estudia la infraestructura de información y, más importante aún, la manera como dicha infraestructura se usa en el día a día. En OCTAVE se considera que, con el fin de que una organización pueda cumplir su misión, los empleados a todo nivel necesitan entender qué activos relacionados con la información son importantes y cómo deben protegerlos; para ello, es fundamental que en la evaluación estén directamente involucradas personas de diferente nivel de la organización.

OCTAVE es un estudio auto dirigido, desarrollado por un equipo interdisciplinario llamado *el equipo de*

2 El CERT es un centro de investigación en seguridad en Internet del Software Engineering Institute (SEI) de la Universidad de Carnegie Mellon.

análisis, el cual se compone de personas de las áreas de negocio y del área de TI. Esta composición se explica con el hecho de que los funcionarios del negocio son los más indicados para identificar qué información es importante en los procesos del día a día y cómo se usa dicha información; por su parte, son las personas del área de TI las que conocen los detalles de configuración de la infraestructura y las debilidades que puede tener. Estos dos puntos de vista son importantes para tener una visión global de los riesgos de seguridad de los servicios de TI.

El equipo de análisis debe identificar los activos relacionados con la información que son de importancia para la organización, entendiendo esta importancia en términos de que se garantice la continuidad de operación. El análisis se focaliza sobre los activos que se identifican como críticos y la identificación del modo en que se relacionan dichos activos entre sí, las amenazas a las que están expuestos y las vulnerabilidades (organizacionales y tecnológicas). El estudio se hace desde un punto de vista operacional, se verifica cómo se usan los diferentes activos y cómo pueden estar en riesgo debido a amenazas de seguridad. Finalmente, se define una estrategia basada en prácticas para el mejoramiento organizacional y un plan de mitigación para reducir el riesgo al que está expuesta la organización.

DESARROLLO DE LA EVALUACIÓN

OCTAVE se desarrolla mediante una serie de talleres en los que el equipo de análisis y el personal clave de los diferentes niveles de la organización adelantan el levantamiento y análisis de la información. Este proceso se divide en tres fases:

Fase 1- Construir perfiles de amenazas basados en los activos

Los diferentes miembros de la organización contribuyen con su visión sobre los activos que son críticos para la empresa, la manera como se usan y lo que en la actualidad se está haciendo para protegerlos. El equipo evalúa la información y selecciona los activos más importantes. A continuación, se describen los *requerimientos de seguridad* y se crea un *perfil de amenazas* para cada activo crítico.

La fase 1 se desarrolla en cuatro etapas. Las tres primeras son talleres realizados a diferentes niveles de la organización: directivo, gerencial, operativo y de TI. En cada uno de estos talleres se desarrollan actividades tendientes a identificar los principales activos relacionados con la información, las amenazas que se identifican sobre cada uno de ellos, el impacto que tienen dichas amenazas sobre los mismos y sobre la organización, y los requerimientos de seguridad de cada activo.

En la cuarta etapa se consolida la información recolectada en las etapas 1 a 3, verificando aspectos como la completitud, coherencia y diferencias de apreciación en los diferentes niveles de la organización. La información se analiza y se organiza según las amenazas que se presentan para cada activo. Los talleres que se desarrollan en estas fases giran en torno a discusiones dirigidas, a formatos preestablecidos que se diligencian durante cada taller y a encuestas de prácticas de seguridad en la organización; todos ellos con guías de manejo que tiene la metodología.

Como resultado de esta fase se tendrán, entre otros, los siguientes productos:

- Activos críticos: Se identifican los activos relacionados con la información que son de mayor criticidad para la operación y subsistencia de la organización. Así, por ejemplo, en el hipotético caso de un hospital se podrían identificar como activos críticos el sistema de manejo de historias clínicas de los pacientes, los equipos de cómputo usados por los médicos para acceder al sistema de historias clínicas y las historias clínicas en sí mismas[3].
- Requerimientos de seguridad para los activos críticos: Se identifican los aspectos que son importantes de proteger para cada activo. Típicamente se

3 Esto teniendo en cuenta que puede haber consideraciones de tipo legal que obliguen a garantizar la confidencialidad de esta información

consideran aspectos de confidencialidad, integridad y disponibilidad. En el caso anterior, para el sistema de manejo de historias clínicas, se tendría la disponibilidad como principal requerimiento para poder garantizar la atención continua a los pacientes. En el caso de las historias clínicas, la confidencialidad podría ser el principal requerimiento por garantizar y, en el caso de los equipos de los médicos, la disponibilidad.

- Perfiles de amenazas: Un perfil de amenaza es una manera estructurada de mostrar las diferentes amenazas que se presentan sobre cada activo crítico. El perfil de amenazas identifica el actor que genera la amenaza, el motivo u objetivo que perseguiría el actor, la manera como podría acceder al activo (físicamente, a través de la red) y el impacto que generaría sobre el activo y sobre la organización (modificación, destrucción, pérdida, interrupción, vulnerabilidad de la confidencialidad, etc.). OCTAVE identifica cuatro perfiles principales: acceso a través de la red, acceso físico, problemas del sistema y otros problemas.
- Prácticas actuales de seguridad: Se identifican las prácticas de seguridad en la organización. Esta identificación es la base sobre la que se construirá más adelante la estrategia de protección de la empresa. Para ello, OCTAVE incluye una serie de catálogos de prácticas de seguridad que se evalúa en los diferentes talleres, con una herramienta que facilita a los participantes el entendimiento de lo que es una práctica de seguridad y una vulnerabilidad. En el caso del hospital, podrían identificarse vulnerabilidades como la no existencia de políticas claras de seguridad, el manejo inadecuado de contraseñas de acceso a los sistemas y problemas de capacitación y entrenamiento.

Fase 2- Identificar vulnerabilidades en la infraestructura

El equipo de análisis identifica los principales elementos de TI y los diferentes componentes que se relacionan con cada activo crítico. Se evalúan entonces los diferentes componentes para identificar las vulnerabilidades que pudieran facilitar las acciones no autorizadas sobre los activos críticos. Las salidas de esta fase son, entre otras:

- Componentes claves: Se identifican los componentes más importantes que están relacionados con cada activo crítico como firewalls, servidores, routers, sistemas de backup y almacenamiento de información, entre otros; a fin de visualizar todos los caminos de acceso al activo crítico y elementos que se puedan constituir en puntos de acceso no autorizado al activo evaluado.
- Vulnerabilidades tecnológicas actuales: Cada componente es evaluado mediante diferentes técnicas (herramientas de detección de vulnerabilidades, equipo técnico de inspección) para identificar las debilidades que pueden llevar a accesos no autorizados sobre los activos críticos. Es una actividad muy técnica que, incluso, puede ser subcontratada a terceros dentro de la valoración de riesgos.

Fase 3- Desarrollar estrategias y planes de seguridad

En esta etapa el equipo de análisis identifica los riesgos sobre los diferentes activos críticos y decide qué acciones tomar. El equipo crea entonces una estrategia de protección y planes de mitigación, basados en la información recolectada. Las salidas de esta fase son:

- Identificación y evaluación de riesgos: Basados en la información de las etapas anteriores y particularmente en los perfiles de amenazas, se identifican los riesgos y se evalúa el impacto en términos de una escala predefinida (alto, medio, bajo) de acuerdo con los criterios que deben definirse durante las fases anteriores. Estos criterios pueden basarse, a su vez, en aspectos como: pérdidas económicas, afectación de la imagen, generación de riesgo sobre vidas humanas, entre otros. Por ejemplo, en el caso del hospital, una modificación no autorizada sobre una historia clínica puede considerarse como de impacto alto, dado que genera riesgos a la vida de los pacientes, expone al hospital a demandas y puede afectar de manera muy negativa la imagen del centro hospitalario.

- Estrategia de protección y planes de mitigación del riesgo: Se desarrollan los planes de mejora y los próximos pasos para proteger los activos críticos. Se determina qué se va a hacer para implementar los resultados de la evaluación. Esta estrategia se desarrolla a partir de las vulnerabilidades y prácticas de seguridad identificadas durante la fase 1 y 2 de la metodología.

REFLEXIONES ACERCA DE OCTAVE

Existen muchas metodologías para hacer una evaluación de riesgos informáticos. El principal problema al que se está expuesto al hacer una evaluación de este tipo es que no se identifiquen oportunamente riesgos importantes a los que, eventualmente, la organización sea vulnerable. Metodologías como OCTAVE minimizan este problema. Es importante que el análisis se realiza desde la perspectiva del uso que se hace de los sistemas, debido a que la gran parte de los riesgos provienen de las costumbres internas de la organización. Esta visión se complementa al crear los perfiles de amenazas en los que la metodología lleva al grupo a contemplar otros riesgos no identificados en el primer análisis. Es evidente también que una evaluación de riesgos es muy particular para cada organización y que no es sano desarrollar una evaluación de riesgos de una empresa a partir de los resultados obtenidos por una organización diferente.

Es importante mencionar que la evaluación de riesgos se debe aplicar de manera periódica y que parte del éxito de la misma radica en el dominio y habilidades del grupo de análisis para llevarla a cabo. Por esto, es importante que este análisis se desarrolle siguiendo metodologías como OCTAVE, que garanticen una aplicación consistente cada vez que se adelante, así como contar con herramientas, catálogos actualizados y mecanismos de evaluación y seguimiento apropiados. Al respecto podemos mencionar que, antes de pensar en comprar cualquier tipo de equipos o software asociados a seguridad, es necesario haber aplicado alguna metodología de análisis de riesgos para ser efectivos en el control de éstos; de otra forma, la organización puede incurrir en gastos elevados sin realmente establecer mecanismos de seguridad contra los riesgos del negocio.

OCTAVE es un muy buen complemento para implementaciones de metodologías como ITIL o COBIT, en las que la evaluación de riesgos es un componente importante, sin que en ellas sea explícita la manera de adelantar dicha evaluación.

GOBIERNO DE LOS RIESGOS DE TI

Dentro del proceso que se quiere realizar para el análisis de riesgos, una vez que se tiene claro el marco de referencia y la metodología a aplicar para llevar este proceso, es necesario tener unas directrices claras orientadas hacia los procesos de misión crítica dentro de la organización. Es por esta razón que, unido a lo anterior, se hace necesario entender cómo se enmarcan estos estándares y metodologías dentro del gobierno de TI.

Ahora, el impacto de las TI en el mundo empresarial ha concitado un creciente interés por parte de la alta gerencia como un elemento que debe ser gestionado eficientemente para sostener y aumentar la ventaja estratégica de las empresas. Este interés se ha originado fundamentalmente por el rol cada vez más protagónico que están jugando las TI en los procesos misionales de las organizaciones. En este contexto de los negocios, el gobierno de TI se ve enfrentado al reto de desarrollar una gestión que integre diferentes enfoques, prácticas y estándares, de tal manera que el gobierno de TI no sea sólo la aplicación de unos estándares sino que de su aplicación armónica se derive una ventaja estratégica y una continuidad del negocio en forma adecuada.

Bajo esta consideración, el gobierno de TI no es una disciplina aislada sino que forma parte integral del gobierno de la empresa; este último se basa en la aplicación de tres dimensiones clásicas del gobierno corporativo: el cumplimiento legal y regulatorio, el desempeño empresarial y la responsabilidad con

terceros (que en nuestro medio se han denominado prácticas de "Buen gobierno corporativo"). Para mencionar un solo caso como ejemplo, bastaría referirse el sector financiero que, en el cumplimiento de la circular externa 052 de la Superfinanciera (la cual hace referencia a la seguridad de la información bajo criterios de confidencialidad, integridad, disponibilidad, eficiencia, confiabilidad y cumplimiento bajo el estándar ISO 27000 y los 4 dominios de COBIT, enfatizando en 16 de sus procesos) ha llevado a que la seguridad de la información sea un tema central de las juntas directivas, para los administradores y funcionarios. Esto debido a las responsabilidades que se derivan de su aplicación y por las implicaciones que tiene a nivel de la nación, ya que la salud del sistema financiero depende en gran medida de la gestión de TI y en particular a la de riesgos.

Bajo los anteriores preceptos, el objetivo fundamental del gobierno de TI es generar una ventaja estratégica sostenible al negocio con el propósito de generar valor a sus grupos de interés (accionistas, clientes, entre otros). Dentro de este marco se han identificado cinco grandes focos de acción: Desarrollar e innovar modelos de negocios que transformen la organización; facilitar el desarrollo y crecimiento de la empresa; aumentar el valor de la empresa; optimizar la operación empresarial; y minimizar los riesgos en la

Componente del gobierno de TI	Objetivo del componente	Herramientas principales que apoyan el componente	Prácticas más difundidas en la utilización de las herramientas	Manifestaciones de buen uso a nivel empresarial
Alineación estratégica	Alinear estrategia de TI con la corporativa	IT-BSC (Balance scorecard de tecnologías de información)	1. Desarrollar e innovar con modelos de negocios que transformen la organización. 2. Facilitar el desarrollo y crecimiento de la empresa. 3. Aumentar el valor de la empresa. 4. Optimizar la operación empresarial. 5. Minimizar los riesgos en la operación de la empresa.	Aumento de la ventaja competitiva
Promesa de valor	Es la oferta que se hace al cliente sobre los beneficios que éste recibe de la relación con la organización	Mapas estratégicos IT-BSC CMMI (Capability Maturity Model Integration) en calidad de software	Productos Servicios Oportunidad de entrega Calidad de los productos y servicios	Diferenciación de soluciones productos y servicios. Menor costo. Mejor satisfacción del cliente. Mejora en el retorno de la inversión.
Gestión del riesgo	Salvaguardar los activos de TI y la recuperación de desastres	COBIT (Control Objectives for Information and relatedTechnology) ISO 27000 Octave	Mitigar, transferir, eliminar y aceptar el riesgo	Coadyuvar a la continuidad de la operación. Minimizar los siniestros
Gestión de recursos	Optimizar el conocimiento, infraestructura, personas, procesos, aplicaciones, instalaciones, datos, información	ITIL CMMI	Mejorar procesos y sincronizar la operación Mejorar los Ciclos de vida de Hw, Sw y servicios	Sincronización de la operación. Mejora en los Acuerdos de niveles de servicio.
Evaluación de desempeño	Seguir los proyectos y monitorear el servicio de TI	CobiT BSC		Mejora de los indicadores de: Factores claves de éxito (KSF) Indicadores de rendimiento claves (KPI) Indicadores de logro claves (KGI)

Tabla 1. Resumen de componente, objetivos y herramientas más difundidas de gobierno de TI

operación de la empresa. Estos cinco objetivos se ven desarrollados por los siguientes componentes sobre los cuales se centra el gobierno de TI: alineación estratégica, promesa de valor, gestión del riesgo, gestión de recursos y evaluación de desempeño, los cuales no deben ser gestionados independientemente sino armónicamente como se ilustra en la Tabla 1.

Como recomendación, mencionamos que la aplicación de estándares o métodos sin una visión estratégica clara es el gran riesgo que se corre al aplicar de forma independiente o en forma desarticulada, los diferentes modelos o metodologías, los cuales se vuelven un fin en sí mismos y que no tengan un foco estratégico claro. La visión del riesgo, los estándares y la metodología OCTAVE, enmarcados dentro de una visión común y relacionados con los modelos que se han ilustrado anteriormente, son esfuerzos que deben ir en la dirección correcta. En particular, la identificación de activos críticos y la forma de mitigar los riesgos no son independientes, sino que depende de la forma en que construyen valor a la organización y determinan el rol de las TI.

CONCLUSIONES

Es claro que las organizaciones hoy en día son conscientes de la necesidad de identificar los riesgos asociados a TI, pero también es claro que al tener esta preocupación y no aplicar una metodología adecuada para cada negocio (es decir, entendiendo su cultura organizacional, sus procesos, sus operaciones de misión crítica) es imposible lograr que estas metodologías alcancen sus metas de minimizar los riesgos. Es por esta razón que, adicionalmente a conocer los estándares, normas, regulaciones y metodologías de análisis de riesgos, es necesario contar con un gobierno de TI que establezca en forma clara las directrices estratégicas para llevar en forma exitosa estos procesos de análisis de riesgos. Lo anterior significa que para lograr un proceso exitoso se requiere de la sinergia del conocimiento de los estándares y normas, con las metodologías a aplicar y con un gobierno de TI que lidere, organice y defina los lineamientos a seguir, con miras a sostener sus procesos de misión crítica bajo una cultura organizacional.

REFERENCIAS BIBLIOGRÁFICAS

[1] "Getting smarter about IT Risk: The Economist".
Economist Intelligence Unit. The Economist - Hewlett Packard, 2008.

[2] G. Westerman and R. Hunter,
IT Risk: Turning Business Threats into Competitive Advantage. Boston: Harvard Business School Press, 2007.

[3] Dirección de Comunicaciones Corporativas – Bancolombia.
"Sala de prensa. Grupo Bancolombia". Fecha de consulta 1 de abril de 2010. Disponible en: http://www.grupobancolombia.com/home/saladeprensa/noticias/2010/2010-infoSaldos.asp, 2010

[4] J. Santa.
Análisis de marcos de gestión del riesgo de TI: Los marcos 4A, Risk IT y la construcción de una herramienta de análisis. Bogotá: s.n., 2009.

[5] D. Murali.
"Create a risk-aware IT behaviour. *The Hindu* Business Line". The Hindu, 2008. Fecha de consulta: 1 de abril de 2010. Disponible en: http://www.blonnet.com/ew/2008/12/15/stories/2008121550190400.htm.

[6] J. Pinzón.
Acercamiento a la Gestión de Riesgos con Magerit y las 4A. Bogotá: s.n., 2009.

[7] G. Stoneburner, A. Goguen and A. Feringa.
Risk Management Guide for Information Technology Systems. NIST SP 800-30. Department of Commerce, Unite States of America. July 2002. Fecha de consulta: 1 de abril de 2010. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[8] *Enterprise Risk: Identify, Govern and Manage IT Risk*. 2009. Risk IT. IT Governance Institute. Fecha de consulta: 1 de abril de 2010. Disponible en: http://www.isaca.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=47967.

[9] CERT.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). CERT - Software Engineering Institute - Carnegie Mellon University. September 17, 2008. Fecha de consulta: 1 de abril de 2010. Disponible en: http://www.cert.org/octave/.

[10]. Consejo Superior de Administración Electrónica.

MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. - España. Fecha de consulta: 1 de abril de 2010. Disponible en: http://www.csae.map.es/csi/pg5m20.htm.

[11] A. Christopher and D. Autrey.

Managing Information Security Risks. The OCTAVE Approach. S.L.: Addison-Wesley, 2003.

[12] A. Christopher and D. Autrey.

OCTAVE Criteria Versión 2.0. Pittsburgh: Carniege Mellon – Software Engineering Institute. December 2001.

[13] B. Miroslav.

The risk assessment of information system security. University of Zagreb, Faculty of Organization and Informatics, Varašdin, Croatia. Fecha de consulta: 1 de abril de 2010. Disponible en: http://www.carnet.hr/CUC/cuc2004/program/radovi/a5_baca/a5_full.pdf.

BIBLIOGRAFÍA

D. Pérez.

"De la Administración al Gobierno de TI", *Revista Sistemas*. No. 96, Asics. 2008, pp. 65-72.

F. Scalone.

Estudio comparativo de los modelos y estándares de calidad del software. Tesis de Magister. Buenos Aires: Universidad Tecnológica Nacional, Facultad Regional, 2006.

Hoestra A, Conradie N.

How to use them in conjunction, PricewaterhouseCoopers.

ISACA

North America 2005 Msc Carlos Zamora Sotelo, Cisa, CISM, CobIT, ITIL, and ISO 17799

ISACA.

COBIT 4.1. Fecha de consulta: 1 de abril de 2010. Disponible en: http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/Obtain_COBIT.htm

IT Governance Institute.

Board briefing on IT governance. 2nd Edition. USA: 2003.

J. Raggio.

Desarrollo de procesos de gestión de servicios de explotación siguiendo el modelo CMMI. Madrid: Universidad Politécnica de Madrid, Facultad de Informática, Estudios de Doctorado,

M. Biegstraaten.

"IT governance para la gestión de servicios: Cobit en la práctica". AC Forum-BMC. Fecha de consulta: 1 de abril de 2010. Disponible en: http://www.bmc.com/es_ES/presentations/Presentacion_CobiT_vs_ITIL_BMC_020306.pdf

Recibido 30 de Abril de 2010, modificado 20 de Agosto de 2010, aprobado 23 de Agosto de 2010.