Artículo **Revista de Tecnologías de la Información**
Diciembre 2014 Vol.1 15-29

Gobierno y riesgos de TI

SOLARES- Pedro†

Universidad Iberoamericana.

Recibido 23 de Enero, 2014; Aceptado 25 de Julio, 2014

Resumen

El término "gobernanza" describe la capacidad de una organización para controlar y regular su propio desempeño con el fin de evitar conflictos de interés, relacionados con la división entre los beneficiarios y los actores de la gobernanza de TI. Derivado de Gobierno Corporativo, y principalmente en la relación entre las empresas y la administración de TI de una organización. Resalte la importación de los asuntos relativos a las TI en las organizaciones modernas y recomienda que las decisiones de TI estratégicas son tomadas por el más alto nivel de directivas. El Instituto de Gobernanza Tecnología de la Información (ITGI) fue establecido en 1998 por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) con el fin de avanzar en el pensamiento y las normas internacionales en la dirección y control de las empresas de tecnología de la información. De acuerdo con el gobierno de TI ITGI es considerado como crítico y como una disciplina de gestión dentro de las empresas públicas o privadas. El gobierno de TI eficaz ayuda a apoya los objetivos de negocio, maximiza la inversión empresarial en TI, y apropiadamente gestiona IT-relacionados oportunidades y riesgos. Estos riesgos incluyen consecuencias legales y financieras en caso de incumplimiento de las leyes Corporativas financieros. Los principales objetivos del Gobierno de TI son: (1) la garantía de que las inversiones en TI generan valor para el negocio y (2) mitigar los riesgos asociados a ella. Esto se puede lograr a través de la implementación de una estructura organizacional con funciones bien definidas para las funciones de información, procesos de negocio, aplicaciones, infraestructura, etc .. Tienen varias mejores prácticas, normas, certificaciones y gobierno de TI riesgos.

Riesgos, Gobierno, TI.

Abstract

The term "governance" describes the ability of an organization to control and regulate their own performance in order to avoid conflicts of interest, related to the division between the beneficiaries and the IT Governance actors. Derived from Corporate Governance, and mainly on the relationship between business and IT management of an organization. Highlight the import of matters concerning IT in modern organizations and recommends that strategic IT decisions are made by the highest level of directives. The Institute of Information Technology Governance (ITGI) was established in 1998 by the Audit Association and Control Information Systems (ISACA) in order to advance international thinking and standards in directing and controlling the information technology companies. According to ITGI IT governance is regarded as critical and as a management discipline within public or private companies. Effective IT governance helps to supports the business goals, maximizes business investment in IT, and appropriately manages IT-related opportunities and risks. These risks include legal and financial consequences for non-compliance with financial corporatives laws. The main objectives of IT Governance are: (1) ensuring that investments in IT generate business value and (2) mitigate the risks associated with IT. This is achievable through the implementation of an organizational structure with well-defined roles for information functions, business processes, applications, infrastructure, etc.. They have several best practices, standards, certifications and government IT risks.

Risks, Governance, IT.

Citación: SOLARES- Pedro Gobierno y riesgos de TI. Revista de Tecnologías de la Información 2014, 1-1:15-29

† Investigador contribuyendo como primer autor.

Artículo **Revista de Tecnologías de la Información**
Diciembre 2014 Vol.1 15-29

Introducción

Un concepto importante para el alineamiento de la Tecnología de Información (TI) con el Negocio es Gobierno o Gobernanza de TI. Gobierno se basa en la palabra del Latín 'gubernare' (dirigir o conducir), por lo tanto es el conjunto de responsabilidades y prácticas ejercitadas por la junta y la dirección ejecutiva con las metas de proporcionar dirección estratégica, asegurar que los objetivos sean alcanzados, determinar que los riesgos se gestionen de forma apropiada y verificar que los recursos de la empresa se asignen y aprovechen de manera responsable.

El Gobierno de TI se define como una disciplina relativa a la forma en la que la alta dirección de las organizaciones dirige la evolución y el uso de las tecnologías de la información. Se considera una parte del denominado "Gobierno Corporativo", centrada en el rendimiento, riesgos y control de las Tecnologías de Información.

El IT Governance Institute de ISACA describe: "El Gobierno de TI como la responsabilidad del Consejo de Administración y la alta dirección. Es una parte integral del Gobierno corporativo y consiste en que el liderazgo, las estructuras organizativas y los procesos aseguren que la TI sostiene y extiende los objetivos y estrategias de la Organización"[13].

Por tanto, el Gobierno de TI tiene que ver, sobre todo con la capacidad de la toma de decisiones, la supervisión y el control de las tecnologías de información.

Gobierno de TI

Actualmente, los sistemas de Gobierno de las TI (IT Governance) se encuentran implantados con éxito en otros sectores (banca, seguros, industria, etc.) alcanzando una madurez de 2,67 sobre 5 en la escala propuesta por el IT Governance Institute (ITGI). También se están incorporando al gobierno de las TI universidades de todo el mundo, y según el estudio realizado por Yanosky y Borreson (2008) ya alcanzan una madurez de 2,30 sobre 5, lo que significa que las universidades se encuentran todavía en una situación incipiente y en proceso de maduración.

Los elementos que favorecen la efectividad del gobierno de las TI no suelen ser estructurales o relacionados con los procedimientos sino que están relacionados con las personas: el apoyo de los directivos, las destrezas y las capacidades personales y la participación e implicación de todos los grupos de interés.

La administración de las TI se vuelve cada vez más compleja pero al mismo tiempo crece en importancia; según Dahlberg y Kivijarvi (2006), algunos de los motivos son:

- La dirección desearía mejorar la rentabilidad del uso de sus recursos de TI. Quiere asegurar que las inversiones en TI proporcionen valor a su negocio y estén alineadas con la consecución del resto de objetivos de la organización.

- Se demandan informes que establezcan cual es la mejora en relación con las TI y se necesita que las TI cumplan con las nuevas necesidades de gestión de la organización.

[13]IT Governance Institute, [En línea]. Disponible en http://www.isaca.org/About-ISACA/IT-Governance-Institute/Pages/default.aspx; Internet; accesado el 1 de Abril de 2014.

ISSN-2410-4000

- La gestión corporativa y las acciones de medida del desempeño han liderado la petición de que las TI deberían gestionarse con prácticas similares a las que se utilizan para otras funciones, como puede ser el Cuadro de Mando Integral (CMI) o el apoyarse en proveedores en relación con la estrategia de la organización.

- Los proveedores de servicios TI y sus usuarios deben medir y gestionar los niveles de servicio, costos, riesgos, etc, de los servicios TI.

Las mejores prácticas de Gobierno de TI son: la ISO 38500, COBIT (Objetivos de Control de TI) 5.0 y la Certificación CGEIT

ISO 38500

La norma ISO/IEC 38500, define el Gobierno de TI como El sistema mediante el cual se dirige y controla el uso actual y futuro de las tecnologías de la información. Los autores Peter Weill y Jeanne Ross, en su libro IT Governance, menciona la siguiente definición: "Especificación de las capacidades decisorias y el marco de rendición de cuentas para estimular las conductas más adecuadas en el uso de las tecnologías de la información" [14].

Con base en la definición, la norma empieza dejando claro que el gobierno de las TI no es un elemento aislado sino que "es un sistema", conformado por diferentes elementos ("estrategias y políticas"), cada uno de los cuales tiene valor por sí mismo y el valor del sistema que los integra es mayor que el valor de la suma de sus partes (pensamiento sistémico).

El gobierno de las TI sirve para "dirigir y controlar", entendiendo el primer término por tomar decisiones y planificar su ejecución y el segundo como supervisión y evaluación de los resultados. "Se refiere al uso actual y futuro de las TI porque los directivos de la organización se tienen que asegurar que controlan los sistemas en funcionamiento pero no deben olvidarse de disponer de un plan para su funcionamiento futuro y para integrar nuevas tecnologías. Los planes de TI deben dar soporte al plan de negocio de la organización y su meta debe ser alcanzar los objetivos establecidos o lo que es lo mismo buscar el alineamiento con los objetivos de negocio"[15].

Para la implementación de Gobierno de TI se recomienda la norma ISO/IEC 38500 publicada en el mes de junio del año 2008, teniendo como "objetivo principal el proporcionar un marco de principios para que la dirección del negocio se base en ésta para evaluar, dirigir y monitorear el uso de las Tecnologías de la Información; sus principios son"[16]:

- Responsabilidad. Todos tienen que comprender y aceptar sus responsabilidades en la oferta o demanda de TI.

- Estrategia. La estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de las TI.

- Inversión. Las adquisiciones de TI se hacen por razones válidas, basándose en un análisis apropiado y continuo, con decisiones claras y transparentes.

[14]Peter D. Weill and Jeanne W. Ross, IT Governance. Harvard Business Review Press. U.S.A. 2004.

[15]ISO 38500. [En línea]. Disponible en http://www.iso.org/iso/pressrelease.htm?refid=Ref1135, accesado el 30 de abril de 2014

[16]Ibídem.

- Rendimiento. La TI está dimensionada para dar soporte a la organización, proporcionando los servicios con la calidad adecuada para cumplir con las necesidades actuales y futuras.

- Cumplimiento. La función de TI cumple todas las legislaciones y normas aplicables.

- Conducta Humana. Las políticas de TI, prácticas y decisiones demuestran respeto por la conducta humana, incluyendo las necesidades actuales y emergentes de toda la gente involucrada.

- El establecimiento de responsabilidades. A las personas competentes para la toma de decisiones.

- Alineamiento. De las TI con los objetivos estratégicos de la organización.

- La inversión. En bienes de TI adecuados.

- Adquisición. Las adquisiciones de TI se hacen por razones válidas, basándose en un análisis apropiado y continuo, con decisiones claras y transparentes.

- Conformidad. La función de TI cumple todas las legislaciones y normas aplicables. Las políticas y prácticas al respecto están claramente definidas, implementadas y exigidas.

De la misma manera, ésta norma se aplica al gobierno de los procesos de gestión de las tecnologías de la información en todo tipo de organizaciones que utilicen (hoy en día casi un 100%).

Facilitando las bases para la evaluación objetiva del Gobierno de TI.

"Principios de Gobierno de las TI de la norma ISO 38500 Adaptado de ISO 38500 (2008)".

- Responsabilidad. Establecer las responsabilidades de cada individuo o grupo de personas dentro de la organización en relación a las TI.

- Estrategia. Hay que tener en cuenta el potencial de las TI a la hora de diseñar la estrategia actual y futura de la organización.

- Adquisición. Las adquisiciones de TI deben realizarse después de un adecuado análisis y tomando la decisión en base a criterios claros y transparentes. Debe existir un equilibrio apropiado entre beneficios, oportunidades, coste y riesgos, tanto a corto como a largo plazo.

- Desempeño. Las TI deben dar soporte a la organización, ofreciendo servicios con el nivel de calidad requerido por la organización.

- Cumplimiento. Las TI deben cumplir con todas las leyes y normativas y las políticas y los procedimientos internos deben estar claramente definidos, implementados y apoyados.

- Factor humano. Las políticas y procedimientos establecidos deben incluir el máximo respeto hacia la componente humana, incorporando todas las necesidades propias de las personas que forman parte de los procesos de TI.

ISSN-2410-4000

El estándar hace énfasis en el rol fundamental de los Directivos que está en el establecer las políticas y estrategias así como en la monitorear la gestión del cumplimiento con la legislación y normas internas y externas existentes y el rendimiento de los recursos utilizados.

También la norma reconoce que no hay unas grandes expectativas de que los Directivos tengan una gran especialización técnica, por lo que sus decisiones se basarán en el asesoramiento que procederá de sus ejecutivos y de fuentes externas. En aquellos aspectos en los que la TI es crítica para la organización sería factible que los Directivos obtuvieran opiniones independientes de la misma manera que la auditoría financiera es una actividad rutinaria para una gran cantidad de organizaciones.

Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa: COBIT 5.0

"COBIT (Objetivos de Control para las Tecnologías Relacionadas con la Información) 5.0 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas.

COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público"[17].

"COBIT 5.0 es un marco de referencia único e integrado porque"[18]:

- Se alinea con otros estándares y marcos de referencia lo que permite usarlo como el marco integrador general de gestión y gobierno.
- Es completo en la cobertura de la empresa, ofreciendo una base para integrar de manera efectiva otros marcos, estándares y prácticas utilizadas.
- Proporciona una arquitectura simple para estructurar los materiales de guía y producir un conjunto consistente.
- Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA.

COBIT 5 ofrece principios, prácticas, herramientas analíticas y modelos globalmente aceptados para ayudar a los directivos de negocio y de TI a maximizar la confianza en el valor de sus activos tecnológicos y de información.

Empresas de todo el mundo necesitan una guía para gobernar, gestionar y asegurar la obtención de valor a partir de las vastas cantidades de información que manejan y las rápidamente cambiantes tecnologías que emplean.

[17]Un marco de negocio para el gobierno y la gestión de las TI de la empresa, [En línea]. Disponible en http://www.isaca.org/COBIT/Documents/COBIT5-Framework-Spanish.pdf, accesado el 29 de abril de 2014.
[18]Un recorrido por COBIT 5.0, [En línea]. Disponible en http://www.isacacr.org/archivos/UN%20RECORRIDO%20POR%20COBIT%205%20%2019-06-13.pdf, accesado el 29 de Abril de 2014.

COBIT 5 ofrece una guía para las empresas en la toma de decisiones eficaces, considerando las necesidades de los diferentes grupos de interés.

COBIT 5 tiene la característica de ser adaptado a todos los modelos de negocio, entornos tecnológicos, sectores, geografías y culturas corporativas. Es factible de aplicarse a:

- La seguridad de la información.
- La gestión del riesgo.
- El gobierno corporativo y la gestión de las TI de la empresa.
- Las actividades de revisión y garantía.
- La conformidad legal y regulatoria.
- El tratamiento de datos financieros o de información sobre RSC.

COBIT 5 dota a los profesionales de las herramientas y técnicas definitivas para gobernar las TI corporativas con un enfoque de negocio. El marco COBIT 5 simplifica los retos a los que se enfrenta el gobierno corporativo con tan sólo cinco principios y siete familias de catalizadores. Asimismo, integra otros enfoques y modelos como TOGAF, PMBoK, Prince2, COSO, ITIL, PCI DSS, la Ley Sarbanes-Oxley y Basilea III.

Certificación en Gobierno de TI

La acreditación CGEIT (, orientada a los profesionales implicados en el Gobierno Corporativo de las TIC en las Empresas [y otros organismos/entidades]. El Gobierno de TI ha defendido siempre la naturaleza fronteriza del Gobierno Corporativo de TI:

Es una responsabilidad de los órganos de gobierno y de alta dirección de las organizaciones; pero en su desarrollo y puesta en marcha tienen un papel fundamental los responsables y especialistas de TI. Tomando esta afirmación como punto de partida, la certificación CGEIT está dirigida a los consejos de administración o a equipos de alta dirección de empresas u organizaciones.

En el momento de su creación, ISACA declaraba que CGEIT está orientado, tanto a la gente de negocio, como a la de TI, a comprender la contribución que las TI realizan a la generación de valor para las organizaciones. Los contenidos en el cuerpo de conocimiento de "CGEIT son:(1) marcos de referencia para el Gobierno Corporativo de TI, (2) alineamiento estratégico de TI con el negocio, (3) aporte de valor por parte de TI, (4) gestión del riesgo vinculado a TI, (5) gestión de los recursos de TI y (6) medida del rendimiento de la propia función de TI"[19].

Los contenidos permiten definir la certificación CGEIT, como una certificación profesional afín al CIO y a su "círculo de confianza" (equipo de colaboradores); esto es, una certificación profesional que se adapta perfectamente a los perfiles profesionales de aquellos individuos que intervienen en la buena marcha del Gobierno Corporativo de TI, desde el lado de la oferta: CIO, miembros de oficinas del CIO, encargados de la planificación estratégica de TI, de la gestión de la cartera de TI, de la gestión de los riesgos corporativos derivados del uso de las TI, encargados del márketing de TI, etc.

[19]ISACA, CGEIT - Certified in the Governance of Enterprise IT, [En línea]. Disponible en http://www.ucertify.com/l/es/exams/ISACA/CGEIT.html , accesado el 9 de mayo de 2014

"El programa CGEIT apoya las crecientes demandas y reconoce el amplio rango de profesionales cuyo conocimiento y aplicación de principios de Gobierno de TI son claves para el éxito de un programa de gestión.

La certificación es sinónimo de excelencia y ofrece un número de beneficios tanto a nivel profesional como personal, constituyendo una ventaja competitiva para"[20]:

Las Empresas y Organizaciones:

- Establecer un estándar de mejores prácticas, añadiendo credibilidad y reconocimiento.
- Proveer una orientación a la administración del riesgo en tecnología y en el negocio.
- Actualizar las competencias del personal.
- Facilitar el acceso a una red global de la industria y de expertos en la materia.

Los Profesionales:

- Demostrar conocimiento en Gobierno de TI.
- Vincularse con un programa profesional que tiene aceptación mundial.
- Mejorar sus oportunidades laborales y estabilidad económica.
- Distinguirse como profesional calificado.
- La Certificación es considerada en la actualidad como un reconocimiento de que el profesionista que lo ha obtenido, cuenta con los conocimientos teóricos y prácticos necesarios para desempeñarse adecuadamente.

Riesgos de TI

La definición de Riesgos de Seguridad de la Información con base al estándar internacional ISO/IEC 27005:2011 es: "el potencial de que una cierta amenaza explote vulnerabilidades de un activo o grupo de activos y así cause daño a la organización"[21].

La gestión de riesgos permite a una organización identificar qué necesita proteger, cómo debe protegerse y cuánta protección necesita, y así invertir sus esfuerzos y recursos efectivamente. Para lograr identificar los riesgos es necesario determinar: activos, amenazas, controles existentes, vulnerabilidades, consecuencias e impactos.

Existen diversos marcos de referencia de riesgos, algunos de ellos son:

- ISO 31000
- IEC/DIS 31010
- ISO/D Guide 73
- BS 31100
- ISO/IEC 27005
- ITGI - The Risk IT Framework

[20]Ibídem.

[21]ISO/IEC 27005: 2011 Information technology — Security techniques — Information security risk management (second edition, [En línea]. Disponible enhttp://www.iso27001security.com/html/27005.html; accesado el 25 de abril de 2014.

- Basilea III
- OCTAVE
- NIST SP800-30
- CRAMM
- MAGERIT
- TRA Working Guide
- Microsoft – SRMG
- BS 7799-3
- AIRMIC, ALARM, IRM – ARMS • UNE 71504
- AS/NZS 4360
- M_o_R

Los que tienen mayor demanda son: la ISO 31000 y el ITGI - The Risk IT Framework. A continuación se describen cada uno de ellos.

ISO 31000

La variedad, complejidad y naturaleza de los riesgos es factible ser de muy diversa índole por lo que el Estándar Internacional desarrollado por la IOS (nternational Organization for Standardization) propone unas pautas genéricas sobre cómo gestionar los riesgos de forma sistemática y transparente.

El diseño y la implantación de la gestión de riesgos dependerán de las diversas necesidades de cada organización, de sus objetivos concretos, contexto, estructura, operaciones, procesos operativos, proyectos, servicios, etc.

El enfoque está estructurado en tres elementos claves para una efectiva gestión de riesgos[22]:

- Los principios para la gestión de riesgos.
- La estructura de soporte.
- El proceso de gestión de riesgos.

"La norma ISO 31000 está diseñada para ayudar a las empresas a"[23]:

- Aumentar la probabilidad de lograr los objetivos.
- Fomentar la gestión proactiva.
- Ser conscientes de la necesidad de identificar y tratar el riesgo en toda la empresa.
- Mejorar en la identificación de oportunidades y amenazas.
- Cumplir con las exigencias legales y reglamentarias pertinentes, así como las
- normas internacionales.
- Mejorar la información financiera.
- Mejorar la gobernabilidad.
- Mejorar la confianza de los grupos de interés (stakeholder).
- Establecer una base confiable para la toma de decisiones y la planificación.

[22]ISO 31000 - Risk management – ISO, [En línea]. Disponible enhttp//www.iso.org/iso/iso31000. Accesado el 4 de Mayo de 2014.
[23]ISO 31000 Risk Management | BSI Group, [En línea]. Disponible enhttp://www.bsigroup.com/en-GB/iso-31000-risk-management/, accesado el 6 de mayo de 2014.

- Mejorar los controles.
- Asignar y utilizar con eficacia los recursos para el tratamiento del riesgo.
- Mejorar la eficacia y eficiencia operacional.
- Mejorar la salud y de seguridad, así como la protección del medio ambiente.
- Mejorar la prevención de pérdidas, así como la gestión de incidentes.
- Minimizar las pérdidas.
- Mejorar el aprendizaje organizacional.
- Mejorar capacidad de recuperación de la empresa.

"Para una mayor eficacia, la gestión del riesgo con base en la ISO 31000 en una empresa es factible de tener en cuenta los siguientes principios"[24]:

- Crea valor. Ayudando a conseguir objetivos y mejorar aspectos como la seguridad y salud laboral, cumplimiento legal y normativo, protección ambiental, etc.
- Está integrada en los procesos de una empresa. No debe ser entendida como una actividad aislada sino como parte de las actividades y procesos principales de una organización.
- Forma parte de la toma de decisiones. Ayuda a la toma de decisiones evaluando la información sobre las diferentes opciones.
- Trata explícitamente la incertidumbre. Trata aquellos aspectos de la toma de decisiones que son inciertos, la naturaleza de esa incertidumbre y como puede tratarse.
- Es sistemática, estructurada y adecuada. Contribuye a la eficiencia y a la obtención de resultados fiables.
- Está basada en la mejor información disponible. Las entradas del proceso se basan en fuentes de información como la experiencia, la observación, las previsiones y la opinión de expertos.
- Está hecha a medida. Está alineada con el contexto externo e interno de la empresa y con su perfil de riesgo.
- Tiene en cuenta factores humanos y culturales. Reconoce la capacidad, percepción e intenciones de la gente, que es factible de facilitar o dificultar la consecución de los objetivos.
- Es transparente e inclusiva. La apropiada y oportuna participación de los grupos de interés (stakeholders) y de los responsables a todos los niveles, asegura que la gestión del riesgo permanece relevante y actualizada.
- Es dinámica, iterativa y sensible al cambio. La empresa debe velar para que la gestión del riesgo detecte y responda a los cambios del negocio.
- Facilita la mejora continua de la empresa.

[24] AEC-ISO 31000, [En línea]. Disponible enhttp://www.aec.es/web/guest/centro-conocimiento/iso-31000, accesado el 15 de mayo de 2014.

ITGI - The Risk IT Framework

"El marco de RISK IT está destinado a un público amplio, ya que la gestión de riesgos es una práctica global y un requisito estratégico en cualquier organización. El público objetivo incluye"[25]:

- Los principales ejecutivos y miembros del consejo que necesitan para establecer la dirección y seguimiento del riesgo a nivel de organización.

- Encargados de TI y de los departamentos de negocio que necesitan definir el proceso de la gestión de riesgos.

- Profesionales de la gestión de riesgos que necesitan la dirección específica en cuanto a los riesgos de TI.

- Las partes interesadas externas.

El marco de RISK IT se basa en los principios de gestión de los riesgos organizacionales (ERM), las normas y marcos como COSO ERM 2 y AS/NZS43603, y provee información acerca de cómo aplicar estos principios a las TI. RISK IT aplica los conceptos generalmente aceptados de los principales estándares y marcos, así como los principales conceptos de la gestión de otros riesgos de TI, relacionados con las normas. Aunque RISK IT se alinea con los principales marcos de ERM, la presencia y la aplicación de esos marcos no es requisito previo para la adopción de RISK IT. Mediante la adopción de RISK IT en las organizaciones se aplicarán automáticamente todos los principios de ERM.

En el caso de que ERM esté presente de alguna forma en la organización, es importante aprovechar los puntos fuertes del programa de ERM existente ya que éste ayudará a la organización a la adopción de la gestión de riesgos, a ahorrar tiempo y dinero y a evitar los malentendidos acerca de los riesgos específicos de TI que pueden ocasionar un mayor riesgo en el negocio.

RISK IT se define y se basa en una serie de guías para la gestión eficaz de los riesgos de TI. Dichas guías se basan en los principios comúnmente aceptados en ERM, que se han aplicado en el ámbito de las TI. El modelo del proceso de los riesgos de TI está diseñado y estructurado para que las organizaciones les sea factible poner los principios en práctica y comparar sus resultados.

"El marco de RISK IT se basa en los riesgos de TI. En otras palabras, el riesgo organizacional está relacionado con el uso de las TI. La conexión con la organización se basa en los principios en los que se construye el marco, es decir, el gobierno efectivo de la organización y gestión de los riesgos de TI, Algunos de ellos son"[26]:

- Alinear siempre con los objetivos organizacionales.

- Alinear la gestión de las TI con el riesgo organizacional relacionado con el total de ERM.

- Balance de los costos y los beneficios de la gestión de los riesgos de TI.

- Promover la comunicación abierta y equitativa de los riesgos de TI.

[25] Marco de Riesgos de TI, [En línea]. Disponible enhttp://www.info.unlp.edu.ar/uploads/docs/risk_it.pdf, accesado el 11 de mayo de 2014.

[26]Ibídem

- Establecer el tono correcto desde un enfoque de arriba abajo, definiendo y haciendo cumplir la responsabilidad del personal con los niveles de tolerancia aceptables y bien definidos.

"Mediante la gestión de riesgos de TI, se ha desarrollado un modelo de proceso que les será familiar a los usuarios de COBIT y Val IT. Se facilitan guías sobre las actividades clave dentro de cada proceso, las responsabilidades para el proceso, los flujos de información entre los procesos y la gestión del rendimiento del proceso. El modelo se divide en tres ámbitos: gobernanza del riesgo, evaluación de riesgos y el riesgo de respuesta, cada uno con tres procesos"[27]:

Gobierno de los riesgos (GR)

- Establecer y mantener una vista de riesgo común.
- Integrar con ERM.
- Tomar decisiones conscientes de los riesgos del negocio.

Evaluación de riesgos (RE)

- Recoger datos.
- Analizar los riesgos.
- Mantener perfil de riesgo.

Respuesta de riesgos

- Riesgo articulado
- Manejar riesgos
- Reaccionar a acontecimientos

[27]Marco de Riesgos de TI, op cit.

Certificación en Riesgos

Introducido en 2010, el Certificado en Sistemas de Información de Riesgos y Control (CRISC) es una nueva certificación ofrecida por ISACA y se basa en la propiedad intelectual de la asociación, investigación de mercado independiente y los aportes de expertos en la materia de todo el mundo.

La certificación ha sido diseñada para profesionales de TI y de negocios que identifiquen y gestionen los riesgos mediante la elaboración, implementación y mantenimiento de sistemas adecuados de información de los controles.

"La designación CRISC está diseñado para"[28]:

- Los profesionales de TI.
- Profesionales de riesgo.
- Análisis económico.
- Los gerentes de proyecto.
- Cumplimiento de los profesionales de la empresa.

"La designación CRISC se centra en"[29]:

- Identificación, evaluación y la evaluación de respuestas a los riesgos.
- Supervisión de riesgos.
- Es el diseño de control y aplicación.

[28] CRISC, [En línea]. Disponible enhttp://www.isaca.org/chapters7/Madrid/Certification/Pages/Page4.aspx, accesado el 27 de abril de 2014.
[29] Ibídem.

- Es seguimiento, control y mantenimiento.

CRISC prepara a los profesionales de TI para su crecimiento profesional futuro al vincular la administración de riesgos de TI con la administración de riesgos empresariales. Los profesionales de una amplia gama de funciones que incluye a TI, seguridad, auditoría y el cumplimiento regulatorio han obtenido la certificación CRISC desde que se estableció en abril de 2010. Hasta la fecha, más de 16,000 profesionales cuentan con ella. De estos profesionales, más de 1,200 son CIO, CISO y directores de cumplimiento, riesgos y privacidad.

Cada empresa tiene que seleccionar la metodología que cumpla con sus requerimientos y objetivos. Sin embargo, si hay que especificar un proceso estructurado y sistemático para gestionar riesgos.

Dentro del Gobierno Corporativo la Administración de Riesgos relacionados con la Tecnología de Información está siendo atendida y entendida como un aspecto clave del negocio y el Gobierno de TI se está volviendo cada vez más importante por ser parte integral del éxito de la empresa al asegurar mejoras medibles, eficientes y efectivas de los procesos de TI relacionados con la empresa.

Conclusiones

El gobierno de las TI es una parte integral del gobierno corporativo, entendido como un conjunto de prácticas y responsabilidades ejercidas por el consejo de administración y consejo de dirección de la corporación, con el objetivo de proporcionar una dirección estratégica, asegurar que los objetivos son alcanzados.

Facilitar que los riesgos son gestionados adecuadamente y verificar que los recursos de la organización son utilizados de manera responsable, teniendo en cuenta las demandas de los diferentes grupos de interés, y la continua evolución del entorno corporativo.

En este contexto, el gobierno de las TI comprende el liderazgo, las estructuras organizativas y los procesos que aseguran que las TI de la organización sostienen y extienden los objetivos y estrategias de la misma.

Gobierno de TI es la responsabilidad que tiene la alta dirección de asegurar que las tecnologías de información sustenten los objetivos y estrategias del negocio.

El Gobierno de TI es una representación simplificada, esquemática y conceptual que proporciona un marco de trabajo para:

- Alinear objetivos de TI con el Negocio.
- Generar y mantener valor.
- Administrar los riesgos a un nivel aceptable.

El gobierno de las TI guía la forma de generar valor para la organización y sus grupos de interés, y minimizar los riesgos, a través de la alineación de la estrategia, la gestión de los recursos necesarios, y el desarrollo de herramientas para la medición y comunicación de las diferentes facetas del desempeño. El uso eficiente y eficaz de las TI es factible de generar valor en la organización. Las herramientas (estándares y certificaciones) de qué disponen las organizaciones para conseguir la alineación de la estrategia de TI con la estrategia general de negocio de la organización (y cómo esta alineación genera valor).

ISSN-2410-4000

Para la construcción de medidas e indicadores apropiados que permitan guiar a los responsables y puestos directivos en el control e implantación de la estrategia de TI, y para una adecuada coordinación de los recursos con los que cuenta o es factible de contar mediante su adquisición una organización.

Todas las organizaciones, independientemente de su tamaño o sector, están expuestas a una serie de amenazas que las hacen vulnerables y es factible de entorpecer la correcta consecución de los objetivos establecidos, como son: accidentes operacionales, enfermedades, incendios u otras catástrofes naturales.

El gobierno de las TI es responsabilidad de los miembros del Comité de Dirección y de los altos ejecutivos de la organización.

Esta es una cuestión importante, que deriva de la inclusión del gobierno de las TI dentro del gobierno corporativo, y que sugiere que no se está hablando de la gestión de un departamento de las TI o de la simple provisión de servicios de TI en las organizaciones.

Normalmente los Consejos de Administración carecen de la información adecuada sobre estrategia de TI así como de su gestión. Pero conforme los Consejos se involucran más en las decisiones de TI, comprenden sus roles y profundizan en la definición de la estrategia, las TI son más eficaces en el apoyo del negocio.

En el Gobierno de TI se desarrolla un rol clave tanto del Director General (CEO) como del Director de Información (CIO), especialmente este último, que requiere nuevas competencias, conocimientos y habilidades directivas.

Los ejecutivos de negocio son tan responsables del éxito en el uso y de la gestión de la TI y la consecución de valor para el negocio como el CIO

El principal objetivo del gobierno de las TI es conseguir la alineación entre la estrategia del negocio y la estrategia de las TI. Este proceso es básico para que el gobierno de las TI cumpla su función primordial de generación de valor para los grupos de interés, minimizando los riesgos. El gobierno de las TI incluye estrategias, políticas, responsabilidades, estructuras y procesos para la utilización de las TI en una organización. La inclusión de elementos operativos y elementos estratégicos (de presente y de futuro) es un aspecto esencial del gobierno de las TI, y guía el desarrollo de las tareas de gestión y administración. Gobierno y gestión (o administración) no deben confundirse, porque el primero establece los sistemas y las políticas que sirven de guía y control al segundo.

Para el Gobierno de las TI la alineación supone algo más que la integración estratégica entre la (futura) organización de las TI y la (futura) organización de la empresa. También implica que las operaciones de las TI estén alineadas con las operaciones empresariales en curso.

Por supuesto, es difícil lograr la alineación de las TI cuando el modelo de negocio no está claramente integrado y compartido en las diferentes unidades y áreas que forman la organización.

Las organizaciones tienen que gestionar el riesgo que en un momento dado pueda afectar e impactar negativamente en sus actividades y procesos, lo cual pondría en peligro la consecución de sus objetivos.

ISSN-2410-4000

En el ámbito de las TI, es necesario analizar cómo preservar el valor del negocio a través de la seguridad que les proporcione las TI para proteger sus activos, conservar la continuidad de los servicios y recuperarlos después de un desastre. Pero al diseñar sus estrategias futuras también deben evaluar los nuevos riesgos que aparecen a partir de la incorporación de las TI en los procedimientos y estrategias de la organización.

Desde el punto de vista estratégico, una adecuada gestión de los riesgos conlleva preservar la capacidad del negocio para obtener resultados a medio y largo plazo. La dirección de la organización es responsable de utilizar y/o dotarse de las capacidades y competencias que requiere para desplegar su estrategia y alcanzar los objetivos últimos plasmados en su misión.

Otro aspecto fundamental de la gestión del riesgo es procurar la continuidad de las operaciones que aseguren el rendimiento de la organización y conserven su habilidad para alcanzar sus objetivos a medio y corto plazo.

Para ello, es factible utilizar mecanismos (ISO 31000 y el CRISC entre otros) de gestión de la continuidad del negocio, que identifiquen accidentes potenciales que amenacen a la organización y formulen e implementen estrategias viables de continuidad.

Referencias

AEC-ISO 31000, [En línea]. Disponible en http://www.aec.es/web/guest/centro-conocimiento/iso-31000, accesado el 15 de mayo de 2014.

CRISC, [En línea]. Disponible en http://www.isaca.org/chapters7/Madrid/Certification/Pages/Page4.aspx, accesado el 27 de abril de 2014.

Dahlberg, T. y Kivijarvi, H. (2006).An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument. Proceedings of the 39th Hawaii International Conference on System Sciences. IEEE Computer Society.

Fernández Martínez, Antonio y Faraón Llorens Largo. Gobierno de las TI para universidades, [En línea]. Disponible en http://www.crue.org/Publicaciones/Documents/Gobierno%20TI/gobierno_de_las_TI_para_universidades.pdf, accesado el 5 de mayo de 2014.

Fernando, Solares Valdes, Tesis-. Instrumentación de Gobierno de Tecnología de Información en una Institución Pública, Universidad La Salle Pachuca. 2010.

ISACA, CGEIT - Certified in the Governance of Enterprise IT, [En línea]. Disponible en http://www.ucertify.com/l/es/exams/ISACA/CGEIT.html, accesado el 9 de mayo de 2014

ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition, [En línea]. Disponible en http://www.iso27001security.com/html/27005.html; accesado el 25 de abril de 2014.
ISO 31000 Risk Management | BSI Group, [En línea]. Disponible en http://www.bsigroup.com/en-GB/iso-31000-risk-management/, accesado el 6 de mayo de 2014.

ISO 31000 - Risk management – ISO, [En línea]. Disponible en http//www.iso.org/iso/iso31000. Accesado el 4 de Mayo de 2014.

ISO 38500. ISO/IEC 38500:2008 Corporate Governance of Information, [En línea]. Disponible en Technology. http://www.iso.org/iso/pressrelease.htm?refid=Ref1135, accesado el 30 de abril de 2014.

IT Governance Institute, [En línea]. Disponible en http://www.isaca.org/About-ISACA/IT-

Governance-Institute/Pages/default.aspx; Internet; accesado el 1 de Abril de 2014.

Marco de Riesgos de TI, [En línea]. Disponible en http://www.info.unlp.edu.ar/uploads/docs/risk_it.pdf, accesado el 11 de mayo de 2014

Peter D. Weill and Jeanne W. Ross, IT Governance. Harvard Business Review Press. U.S.A. 2004.

Un marco de negocio para el gobierno y la gestión de las TI de la empresa, [En línea]. Disponible enhttp://www.isaca.org/COBIT/Documents/COBIT 5-Framework-Spanish.pdf, accesado el 29 de abril de 2014.

Turban, E., Leidner, D., McLean, E., Wetherbe, J. (2008). Information Technology For Management: Transforming Organizations In The Digital Economy, 6th Ed. Wiley.

Yanosky, R. Y Borreson Caruso, J. (2008).Process and Politics: IT Governance in Higher Education. ECAR Key Findings. EDUCASE, [En línea]. Disponible en http://net.educause.edu/ir/library/pdf/ekf/EKF0805.pdf, accesado el 9 de Mayo del 2014