Riesgos relacionados al usuario final

Risks related to the end user

Mario Roberto Monges Olmedo

Artículo Recibido: 27/01/2016

Aceptado para Publicación: 05/02/2016

Resumen: La participación del usuario final en los procesos de tecnologías de la información es clave ya que puede salvaguardar con políticas y reglas como poner en peligro la información directa o indirectamente. Es clave identificar esos riesgos que pueden ser relacionados al usuario final de manera a analizar el impacto de los mismos sobre los activos de la información. Una vez que se tiene este análisis se puede hacer una evaluación de riesgo de manera a poder incluir controles ya sea correctivo o preventivo a los procesos de las tecnologías de la información.
Palabras claves: Riesgo, Usuario final, Gestión, Análisis de Impacto, Evaluación de Riesgo

Abstract: The participation of the end user in the processes of information technologies is key since it can safeguard with policies and rules as to endanger the information directly or indirectly. It is key to identify those risks that can be related to the end user in order to analyze their impact on the information assets. Once you have this analysis you can do a risk assessment so that you can include controls either corrective or preventive to the processes of information technologies.

Keywords: Risk, End User, Management, Impact Analysis, Risk Assessment

Introducción

Para el funcionamiento del negocio de las empresas, es importante medir el impacto adverso de los riesgos que se corre en los procesos de las tecnologías de la información . Primeramente se debe partir de la misión y visión de la empresa, de manera a no perder el foco y mantener alineados a los objetivos de las tecnologías de la información con los objetivos del negocio. A su vez, entender la percepción del usuario final con respecto al riesgo puede ayudar a mejorar el desarrollo del tratamiento del riesgo . Con esa base, se apunta a describir el impacto adverso de los riesgos en caso de no cumplir con cualquiera de los siguientes requerimientos básicos de la información del negocio: integridad, disponibilidad y confidencialidad .Integridad se refiere a la realización de cambios no autorizados por parte del usuario final donde este tenga campo de acción; el impacto de este riesgo podría desencadenar en uso erróneo y continuo de la información con datos corrompidos, un sistema contaminado por datos

eróneos que termina en violación integridad y también confiabilidad de la misma. Disponibilidad es tener la información necesaria cuando se la precisa; en caso de que no se cumpla con este requisito se pueden fallar en cumplir con algunos o varios objetivos de la empresa al no tener la información requerida para completar alguna tarea de algún sistema crítico y esto a su vez puede desencadenar pérdida de tiempo productivo, falta de respuestas concretas y precisas de los usuarios finales, y por ende la toma de decisiones incorrectas por la gerencia. La confidencialidad es clave cuando recae sobre el usuario final ya que este debería proteger uno de los activos más importantes de la empresa hoy en día que es la información; el impacto de no cubrir este requerimiento puede resultar en la divulgación no autorizada, lo que puede caber en faltas graves para el negocio como pérdida en la confidencialidad pública, pérdida de ventaja contra los competidores del ramo, hasta se pueden llegar a tomar esas filtraciones no autorizadas como para hacer pasar vergüenza y/o por acciones legales contra la empresa .(ISACA,2013)

En líneas generales, para tener una guía de acción enfocada a los riesgos para todas las partes involucradas, podemos hacer referencia al ISO 22301 en donde se trata del análisis de impacto de negocio y evaluación de riesgo . Las empresas deben desarrollar y mantener un proceso formal junto con toda la documentación pertinente de forma tal a cubrir los siguientes casos: definir el contexto para la evaluación, estándares y el potencial impacto de un incidente disruptivo, tener en cuenta los requerimientos legales y normas de la empresa, desarrollar análisis sistemático que priorice el tratamiento de riesgos y sus costos, establecer el output requerido del análisis de impacto y evaluación de riesgo, y, detallar la necesidad de actualización y confidencialidad en los requerimientos de esta información . (ISACA,2013)

Entonces por un lado tenemos al análisis de impacto del negocio, en donde el proceso de evaluación documentado establecido por la empresa debe definir las prioridades de continuidad y recuperación, objetivos y puntos de focos; además de incluir la evaluación de impacto de actividades disruptivas que soportan a los productos y servicios de la empresa. En sí, el análisis de impacto debe cubrir puntos como, reconocer las actividades que soportan los productos y servicios, en caso de no poder realizar dichas actividades evaluar su impacto a través del tiempo, y luego, definir lapsos de tiempo priorizados para reanudar estas actividades en un nivel mínimo aceptable específico, también identificar dependencias y recursos de apoyo para estas actividades, incluyendo a los proveedores, compañeros tercerizados, usuarios finales y todas las partes involucradas. (ISACA,2013)

Por consiguiente, una vez que se tiene esquematizado y documentado el análisis de impacto se puede proceder a definir, implementar y mantener un proceso de evaluación de riesgo documentado propiamente, que sistemáticamente determine y analice el riesgo de incidentes disruptivos dentro de la empresa. Para poder cumplir con esta finalidad, la empresa debe: determinar riesgos de disrupción de las actividades priorizadas de la empresa y de los procesos, sistemas, información, personas, activos, tercerizados y otros recursos que soportan esas actividades primordiales, sistemáticamente analizar el riesgo, evaluar que riesgos de disrupción relacionados necesitan de tratamiento y, determinar aquellos tratamientos delineados con los objetivos de continuidad del negocio de acuerdo con el nivel de riesgos asumidos por la empresa . Este proceso bien puede desarrollarse de acuerdo con el ISO 31000, que trabaja en una forma más detallada la Evaluación de riesgo, ya que el mismo engloba nuevamente subniveles como identificación de riesgos, análisis de los riesgos y evaluación de riesgos; como un proceso por separado y consecuente tiene al tratamiento de los riesgos , que se esquematiza y contextualiza en el proceso de gestión de riesgo, en la figura 1:

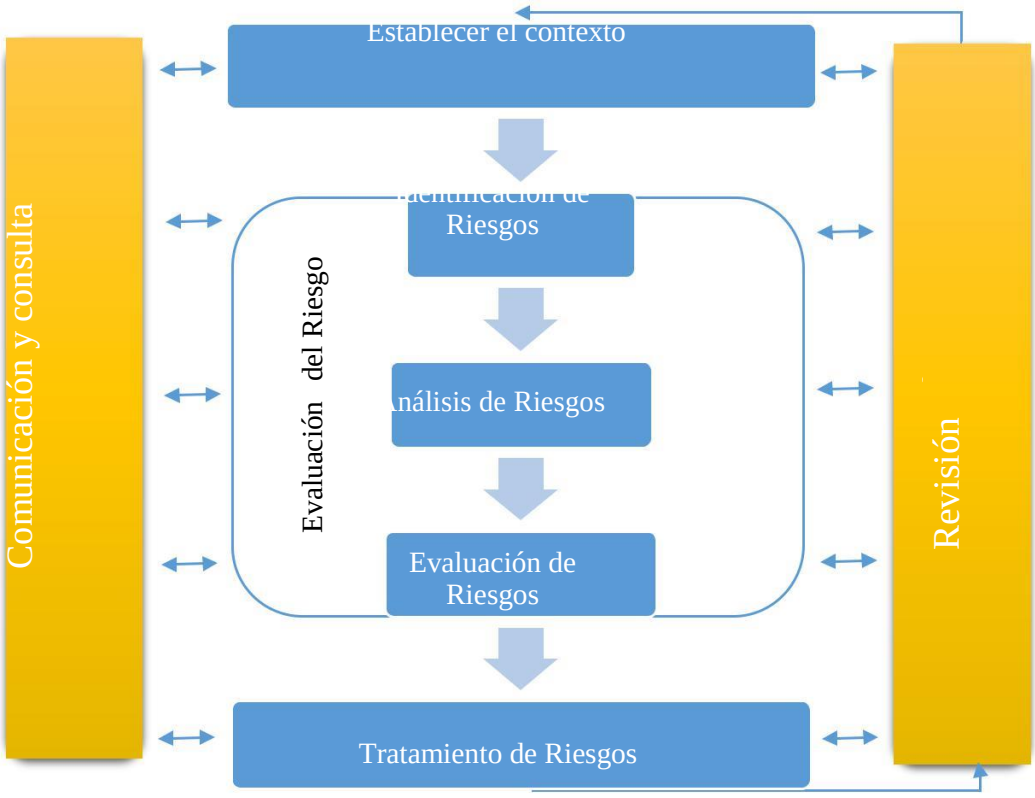

Figura 1: Proceso de Gestión de Riesgo – ISO 31000 [5]

De acuerdo con esta figura del ISO 31000 del proceso de gestión de riesgos, para poder analizar, evaluar y hacer un tratamiento de riesgos, es necesario primero identificarlos. Isaca por su parte es claro en presentar en su material los factores de riesgos relacionados con proyectos de tecnología de la información que pueden servir de guía para identificar aquellos ya bien sabidos, los cuales pueden causar el fracaso en la implementación de nuevas tecnologías, en actualizaciones y modificaciones de sistemas ya existentes o en la reingeniería de procesos de negocios. A continuación una lista de esos factores de riesgo que tienen que ver con el usuario final: falta de recursos calificados, es probable que los usuarios finales no estén capacitados para lidiar y operar con el nuevo o modificado proyecto de tecnología de la información; requerimientos no claros o cambiantes, los usuarios finales pueden componer la lista de las partes involucradas necesarias para definir una de las partes más importantes y básicas del desarrollo del ciclo de vida de los sistemas, que son los requerimientos; resistencia de los usuarios finales, finalmente son ellos los que operan esos sistemas de modo que es necesario no solo capacitarlos sino que partiendo de la base que se diseñan sistemas que cumplen con sus requerimientos y los ayudan realmente en sus tareas, hacerlos comprender de que de eso trata la finalidad del sistema . (ISACA,2013)

También se hace fuerte moción a hacer partícipe al usuario final en el desarrollo de sistemas de información para mitigar riesgos que puede sufrir el proyecto, ya que una de las mayores causas por el que el desarrollo de proyectos de sistemas de información puede fracasar es por la falta de participación del usuario final. Ahora con qué rol o en qué momento es aún un tema bastante contradictorio y no muy claro en las literaturas, algunos afirman que es conveniente que el usuario final se involucre en la etapa de requerimientos, ya que es parte del grupo al cual van dirigidos los objetivos funcionales de tareas del sistema; otros sugieren que los usuarios finales participen activamente en la etapa de revisión de la usabilidad del sistema para que puedan cerciorarse de que el sistema cumpla con las expectativas de los requerimientos, otros en cambio recomiendan que los usuarios finales estén en todas las etapas del desarrollo del ciclo de vida del proyecto de manera a que la satisfacción del usuario sea maximizada .

Cuando un proyecto de tecnología de la información no logra cumplir con los resultados esperados a ser entregados en un tiempo determinado, los riesgos relacionados con ese fracaso pueden afectar de manera importante a la operación del negocio. Por ejemplificar algunos casos más generalizables y básicos de impacto sobre el negocio, estos pueden ser la pérdida de oportunidad o parte del mercado, no poder llegar a cumplir con la demanda de los clientes, la pérdida de ganancias y muchas otras consecuencias tangibles o intangibles. (ISACA,2013)

Por ese impacto fuerte que pueden representan estos riesgos, Isaca identifica 3 áreas de riesgo amplias que se deberían tomar en cuenta para el planeamiento de los proyectos de tecnologías de información: riesgos de diseño, riesgos de implementación y riesgos de operación o rollout. Dadas estas áreas de riesgo y los tipos de riesgo identificados para cada área, de acuerdo a la descripción de cada uno haremos la correlación entre los mismos y si están relacionados aunque sea en parte al usuario final como se muestra en la tabla 1, para después describir los tipos de riesgos que si se relacionen y cómo lo hacen.

Área de Riesgo	Tipo de Riesgo	Relacionado al usuario final
Riesgo de DISEÑO	Riesgo de Sponsor	
	Riesgo de alcance	x
IMPLEMENTACIÓN	Riesgo de habilidad	x
	Riesgo político	x
	Riesgo Liderazgo	
	Riesgo técnico	x
	Riesgo de Transición	x
	Riesgo Personal	x
	Riesgo de alcance	x
Riesgo de OPERACIÓN o ROLLOUT	Riesgo de administración	x
	Riesgo Técnico	x
	Riesgo Cultural	x

Tabla 1: Área de riesgo relacionado al usuario final

En el área de riesgo de diseño, los siguientes tipos de riesgo pueden relacionarse con el usuario final: riesgo de alcance, riesgo de habilidad y riesgo político. En cuanto al

riesgo de alcance, si el alcance no está apropiadamente definido puede acarrear serios problemas y es donde el usuario final puede ayudar o no a delimitar los requerimientos correctamente ya que trabaja día a día en la parte operativa y conoce la dinámica del negocio y las necesidades dentro de la misma; también puede ser una falla de diseño si son excluidos del alcance del cambio algunas tareas existentes y procesos políticamente sensibles que el usuario final bien podría reconocer y de ser así, aportar sobre los requerimientos de los mismos; el riesgo en realidad existe en la percepción del usuario final para estos puntos.

En el riesgo de habilidad es donde se puede notar más la influencia del usuario final ya que si hay ausencia de pensamiento radical y fuera de lo común se pueden estar descartando nuevas soluciones que pudieran explorarse; es muy arbitrario si el usuario puede pensar en grande, lo cual se considera una de las maneras más efectivas para el alto retorno de inversión; y, los participantes que no posean habilidades amplias pueden tener problemas para entender la visión o enfoque del plan, el cual pudiera así estar fuera o más allá de sus habilidades para proponer un buen plan de acción acorde en base a requerimientos completos.

Cuando se menciona a los riesgos políticos se refiere por ejemplo a las partes involucradas que temen perder poder o que son resistentes al cambio y esto puede generar sabotaje o resistencia pasiva por parte de ellos; es fácil perder el control de los rumores una vez que se propagan y generan temor y subversión de los conceptos que se manejan para el proyecto y sus objetivos; lo más probable es que las partes interesadas, como los usuarios finales, resistan el cambio y sean reacios a las nuevas tecnologías y modificaciones a menos que entiendan y acepten de buena manera los beneficios.

El área de riesgo de implementación también puede involucrar al usuario final en los ámbitos de riesgo técnico, riesgo de transición, riesgo de personal y riesgo de alcance. En el riesgo técnico se habla de que las nuevas o modificadas funciones personalizadas del sistema pueden exceder el tiempo disponible o la capacidad de creatividad de las partes involucradas como los usuarios que lo implementan y con esto, retrasos en la implementación pueden revelar que se subestimo la complejidad de del alcance del proyecto. El riesgo de transición puede referirse a la falta de foco en la implementación por pérdida de personal clave que pueden ser usuarios finales que estén capacitados, motivados, sean entendidos de los objetivos del cambio para luego ser reemplazados por otros que no posean estas cualidades ni perciban así el proyecto,

dificultando la implementación en un aspecto u otro, mínimamente en tiempo por ejemplo.

En el riesgo de personal como su nombre lo dice, el personal es el que puede sentirse agotado y aturdido por la carga de trabajo o puede que su percepción decaída pensando en que trabajar en el proyecto no vale la pena. En cuanto al riesgo de alcance en esta área puede que se dé poca importancia a los requerimientos de los recursos humanos necesarios, resultado de un planeamiento pobre, lo que puede conllevar a que miembros del equipo como los usuarios finales, sientan que la magnitud del esfuerzo es avasallante, lo cual puede afectar el proceso y de la implementación en sí. (V. Garg; J. Camp,2012)

En el área de riesgo de operación o rollout es donde se espera los usuarios finales tengan más participación ya que es su área de acción principal, y es por eso que se lo puede relacionar a sus 3 tipos de riesgos: riesgo de administración, riesgo técnico y riesgo cultural. Riesgo de administración debe cubrir y prevenir problemas de comunicación para con los usuarios que puede terminar en sabotaje y resistencia; los sponsors ejecutivos deben proveer entrenamiento suficiente a los usuarios de manera a prevenir una implementación del proyecto sin éxito por ese lado.

En cuanto a los riesgos técnicos se puede encontrar que los usuarios finales no tienen suficiente soporte para desenvolverse con las nuevas funcionalidades; pruebas inadecuadas puede conllevar a problemas operacionales causados por problemas del software; problemas de integridad de datos pueden desencadenar en la no satisfacción del usuario; la percepción de los usuarios acerca de un sistema con fallas puede disminuir su confianza en el mismo. Por último, riesgos de cultura pueden incluir la resistencia del uso del nuevo o modificado sistema en la empresa por falta de convencimiento a los usuarios finales; esa resistencia puede mermar la percepción de los beneficios que ofrece el sistema; por otra parte un entrenamiento efectivo ayuda por lo general en resolver problemas de percepción de los usuarios; entonces el incremento de un comportamiento disfuncional podría evitarse si los usuarios finales entienden bien y cumplen con los objetivos para alcanzar los beneficios. (V. Garg; J. Camp,2012)

Otro punto importante que se debe tomar en cuenta, el cual atraviesa transversalmente a esas áreas de riesgos mencionadas arriba es el riesgo de percepción del usuario final. Entender la percepción del usuario final con respecto al riesgo puede ayudar a mejorar el desarrollo del tratamiento del mismo riesgo . Si bien las empresas pagan a expertos para desarrollar soluciones tecnológicas para cubrir riesgos de

seguridad y privacidad, estas soluciones tecnológicas se encuentran finalmente limitadas en su efectividad por aspectos como restricciones que encuentran los usuarios finales en la usabilidad. Se cree que por la brecha entre modelos mentales de los expertos y los usuarios finales, los sistemas por lo general son diseñados e implementados con expectativas de decisión ideales que pueden en la práctica ser o no ser correspondidos por las decisiones tomadas de los usuarios finales. Es por ello que se tiene una necesidad grande en entender la percepción de los riesgos de los usuarios de manera a construir tratamientos acordes de los mismos.

Conclusión

Este artículo tiene por finalidad encontrar y delimitar en la literatura aquellos aspectos de riesgos más destacables que pueden relacionarse con el usuario final. Esto es de suma importancia para las empresas ya que es la base para finalmente gestionar el riesgo en el manejo de los activos de la información de la empresa. Identificar esos riesgos es el paso previo al análisis de riesgo, evaluación de riesgo y posterior tratamiento de riesgos en donde se busca salvaguardar con soluciones preventivas y correctivas los requerimientos de la información del negocio como la integridad, disponibilidad y confidencialidad de la misma.

Luego de haber encontrado diferentes perspectivas, podemos decir el usuario final tiene un rol incidente directa o indirectamente en el tratamiento de la información del negocio, por lo cual se puede prever medidas para los riesgos que el usuario pueda representar y sufrir con el mismo. Tanto es así que se han establecido delineamientos generales para la mayoría de las empresas por medio de estándares locales y globales que buscan cubrir la gestión de los riesgos tanto con soluciones tecnológicas como manuales.

Es notable como se puede ver que los riesgos relacionados al usuario final se pueden encontrar no solo en las áreas de riesgo de operación o rollout que es su campo de acción, sino también en las áreas de riesgo de diseño y de implementación, de manera a poder prevenir y gestionarlos también en esas áreas sin subestimarlos. Un elemento clave pero no visible que puede prácticamente trazar la línea entre el éxito y fracaso de la gestión de riesgos de los sistemas de información es la forma como los usuarios finales perciben los riesgos de la información de la empresa como uno de los activos más importantes, entiendan la importancia y alcance del tratamiento de los

riesgos y puedan apreciar los beneficios de los sistemas implementados en sus tareas operativas.

Referencias

Amrit; J. V. Hillegersberg; B. V. Diest, Involving End Users to Mitigate Risk in IS Development Projects, *University of Twente, The Nertherlands*, 2012

ISACA, Certified Risk Information Systems Control Review Manual 2013, Isaca, Illinois, 52-70, 2013

ISO, B. S. 22301: 2012, Societal Security. Business Continuity Management Systems. Requirements. *British Standards Institute, London*, 15-19, 2012.

ISO, ISO31000: 2009, Risk Management. Principles and Guidelines, *International Organization for Standardization*, 15-21, 2009.

V. Garg; J. Camp, End User Perception of Online Risk Under Uncertainty. En System Science (HICSS), 2012 45th Hawaii International Conference on, IEEE, 2012.