Evaluación del contexto organizacional en la gestión del riesgo de tecnología de información con un enfoque basado en COBIT

Evaluation of the organizational context in information technology risk management with a COBIT-based approach

Marlene Lucila Guerrero Julio
Grupo de investigación Nuevas Tecnologías, Programa de Ingeniería Industrial,
Universidad de Santander UDES, Colombia
marlene.guerrero@cvudes.edu.co

Carlos Uc Rios
Universidad Internacional Iberoamericana UNINI, México
carlos.uc@unini.edu.mx

doi: https://doi.org/10.36825/RITI.07.14.004

Recibido: Julio 26, 2019
Aceptado: Septiembre 25, 2019

Resumen: Las Tecnologías de la Información y Comunicación (TIC) se han convertido en herramientas fundamentales para apoyar los procesos de negocio. No obstante, su incorporación ha traído nuevas y sofisticadas amenazas y vulnerabilidades. Por ello, la gestión de riesgos en Tecnologías de Información es un factor determinante para garantizar la continuidad del negocio. Una de las primeras actividades que se deben abordar en la gestión de riesgos, es la evaluación del contexto organizacional, que arroja como resultado una comprensión de la empresa en torno a su estrategia para gestionar riesgos y al papel que tienen los empleados en las necesidades de control. En este artículo se definen un conjunto de indicadores basados en los procesos catalizadores de COBIT para determinar el nivel de madurez del contexto organizacional para la gestión de riesgos. Adicionalmente se propone una estrategia enfocada al recurso humano para la evaluación de las amenazas y vulnerabilidades. Los resultados de su aplicación permitieron constatar que a pesar de que se definen políticas en torno a la gestión de riesgos más del 70% de los empleados no las implementa a cabalidad, por lo cual, evaluar el contexto organizacional periódicamente y con indicadores claros es fundamental.

Palabras clave: COBIT*, Contexto Organizacional, Evaluación, Gestión de Riesgos, Tecnología de Información.*

Abstract: Information and Communication Technologies (ICT) have become fundamental tools to support business processes. However, its incorporation has brought new and sophisticated threats and vulnerabilities. Therefore, Information Technology risk management is a determining factor to ensure business continuity. One of the first activities that must be addressed in risk management is the evaluation of the organizational context, which results in an understanding of the company around its strategy to manage risks and the role that employees have in the needs of control. This article defines a set of indicators based on COBIT enablers Processes to determine the level of maturity of the organizational context for risk management. Additionally, a strategy focused on human resources for the threats and vulnerabilities evaluation is proposed. The results of its application made

it possible to verify that although be defines risk management politics, more than 70% of employees do not fully implement them, so evaluating the organizational context periodically and with clear indicators is essential.

keywords: COBIT*, Organizational Context, Evaluation, Risk Management, Information Technology.*

1. Introducción

De acuerdo con [1] y [2], una de las principales preocupaciones del direccionamiento estratégico es el poder determinar hacia dónde va la organización y cuáles son sus metas a largo plazo. La estrategia organizacional parte entonces de la situación actual de la empresa y a través de una serie de condicionamientos, dados por los valores, las políticas y el entorno, plantea como mejorará su competitividad y cuál será la estratagema para la toma de decisiones y el logro de los objetivos de la visión [3][4].

En la actualidad, los planes estratégicos no pueden dejar de involucrar a las tecnologías de la información y comunicación (TIC) [5], toda vez que las TIC se han convertido en la base para gestionar conocimiento y desarrollar estrategias de innovación empresarial [6].

La principal meta de la estrategia en torno a las tecnologías de información y comunicación en una empresa es poder alinear la inversión e incorporación de las TIC con la estrategia empresarial y los objetivos del negocio. Este último aspecto recibe hoy en día el nombre de gobierno corporativo de TI [7] [8].

Una equivocación común de las empresas es considerar que la tecnología por sí misma es una ventaja competitiva [9], ya que esto no se logra si no se implementan prácticas y procesos que permitan maximizar el valor de las TIC en los procesos de negocio. Todos los días surgen nuevas tendencias TIC que implican inversiones considerables, pero que, además, traen consigo nuevas y más sofisticadas amenazas y vulnerabilidades (riesgos).

En consecuencia, la introducción de tecnología trae consigo riesgos que deben gestionarse al interior de sus funciones organizacionales internas. Ejemplo de estos riesgos es la fuga de información, la cual puede causar daño de imagen organizacional o disminuir la confianza de los clientes afectando económicamente el negocio. Un cambio sostenible implica una adecuada gestión de los riesgos asociados con las TIC.

Figura 1. Riesgos asociados con la incorporación de TIC. Fuente: adaptada de [19].

La gestión de riesgos TIC busca llevar los riesgos a un nivel aceptable y garantizar las medidas de control requeridas [10] [11], pero este proceso implica cambios a nivel del contexto organizacional y no sólo de la inversión en tecnología. Los retos para el cambio son grandes e incluyen al factor humano (individuos) y su auto-reconocimiento como fuente de riesgo.

De acuerdo con [12] [13] y [14], el primer paso para la gestión de riesgos asociados con las tecnologías de la información y comunicación es establecer el contexto organizacional, ya que esta actividad permite no solamente identificar las responsabilidades y las funciones en el marco de la gestión del riesgo, sino también repensar a la organización en cuanto a sus características, necesidades, tecnología que utiliza para apoyar sus procesos de negocio, amenazas, entre otros.

Este artículo presenta en primera instancia, una revisión de la gestión de riesgos en tecnologías de la información y la comunicación desde una perspectiva organizacional, con el fin de analizar cómo se encuentra inmersa la evaluación del contexto organizacional al interior de los diferentes estándares e investigaciones internacionales.

Posteriormente, se mostrará como el marco de trabajo COBIT posibilitó, a través de sus procesos catalizadores, el diseño de una propuesta para evaluar el nivel de madurez de una organización en términos de su contexto organizacional desde dos perspectivas, la primera tendiente a evaluar el grado de alineación de las Tecnologías de la Información con su direccionamiento estratégico, y la segunda en función del diagnóstico enfocado al recurso humano de las amenazas y vulnerabilidades relacionadas con las TIC.

Finalmente, se presentará un ejemplo de la puesta en marcha de la propuesta en una de las empresas colombianas en las que fue aplicada, sirviendo como escenario para evidenciar su validez.

2. La gestión de riesgos a nivel organizacional

El aporte de las Tecnologías de la Información y Comunicación como apoyo a los procesos de negocio y la mejora de la competitividad es innegable. Las TIC han provocado diversas transformaciones en la sociedad moderna y su incursión en entornos como la educación, la comunicación, la salud, la construcción, la automatización de procesos, entre otros, ha venido propiciando una mejora significativa en la vida de las personas y de las organizaciones [15] [16]. Diversas industrias a nivel mundial han venido incorporando las TIC en sus servicios y modelos de negocio, con el fin de aumentar sus ingresos y ser competitivos en un mercado cada vez más cambiante.

Según [17] y [18], uno de los principales retos que plantea la incorporación de las TIC en las organizaciones son los riesgos, ya que cotidianamente se encuentran expuestas a atacantes del Ciberespacio o del interior mismo de la empresa que pueden ocasionar amenazas, cuyas implicaciones sean graves y afecten su patrimonio y/o su reputación.

Ernst y Young en [19], recopilan un panorama de los riesgos a los cuales están expuestas las organizaciones por la incorporación de Tecnologías de información y comunicación (ver figura 1). Entre varios escenarios, señala aspectos importantes como la revelación de datos sensibles, la intrusión de software malicioso, la falta de conocimiento del negocio por parte del personal, la tecnología obsoleta, los bajos niveles de servicio y las fallas críticas del sistema.

Los ataques son cada vez más sofisticados, según [19] [20] y [21], cada día las herramientas para los atacantes son mejores y variadas y el rápido crecimiento de las TIC genera más escenarios de riesgo. Ahora bien, teniendo en cuenta la magnitud de los riesgos y que la información que es administrada por las TIC representa la mayoría de los activos de las empresas, es importante manejar un ambiente tecnológico seguro. Es en este punto donde la gestión del riesgo se constituye en un factor fundamental para mitigar el impacto de las amenazas y vulnerabilidades.

La gestión del riesgo de Tecnología de Información y Comunicación, ha sido ampliamente abordada por diversos estándares y *frameworks* a nivel internacional. Guerrero y Gómez en [22], presentaron una revisión en la que se puede destacar la integración de las actividades relacionadas por los principales marcos normativos, llegando a organizar las siete que se presentan a continuación:

- Establecer el contexto organizacional. Actividad relacionada con el entendimiento de la estrategia organizacional en relación con la incorporación de las TIC en el negocio.
- Identificar los activos críticos. Identificación de los niveles de riesgo en cada uno de los activos tecnológicos.
- Identificar y evaluar las amenazas y vulnerabilidades. Especificar las situaciones externas e inherentes que pueden ocasionar riesgos.
- Diseñar los escenarios de riesgo. Ponderar el impacto sobre la organización de cada uno de los riesgos analizados.
- Diseñar las estrategias de tratamiento. Especificar para cada escenario de riesgo las políticas, herramientas y responsables necesarios para enfrentarlos.
- Documentar los resultados y revisar casos. Actividad clave para lograr un aprendizaje.
- Monitorear y controlar. Actividad relacionada con la realimentación y cambio para mantener una mejora continua.

A pesar de que los estándares y *frameworks* en su mayoría ofrecen información sobre las actividades a desarrollar en la gestión de riesgos, es decir el "qué hacer", poco se puede encontrar respecto del "Cómo hacerlo", es decir, herramientas técnicas que puedan orientar a los auditores o consultores en el proceso de relevamiento de información, que permita obtener un panorama concreto de la organización [23]. El propósito de este artículo es precisamente plantear una estrategia para evaluar o establecer el contexto organizacional que es la primera actividad para la gestión de riesgos; y para ello, se soporta en el marco de trabajo de COBIT 5.0.

3. El contexto organizacional y su importancia en la gestión del riesgo de tecnología de información

El establecimiento del contexto organizacional es la primera actividad que debe desarrollar la empresa ante la gestión de riesgos en Tecnologías de Información. Es importante destacar que cada empresa tiene una cultura particular, por lo cual la aplicación de esta actividad requiere de un repensar de la organización en términos de sus necesidades, estrategias de incorporación de TIC, tecnologías que apoyan los procesos de negocio, y responsabilidades del factor humano. El establecimiento del contexto organizacional es una actividad contemplada explícitamente en los *frameworks* planteados por el Estándar Australiano de Administración del Riesgo AS/NZS [24], el Método de Análisis de Riesgos NIST SP800-30 [25] y el Método para la administración del riesgo en la seguridad de la información SP800-39 [26]. La comparación entre lo que plantea cada una de estas guías, posibilitó la unificación de criterio sobre las subactividades relacionadas con esta actividad y sobre los elementos que se debían tener en cuenta para llevarla a cabo al interior de la organización.

Como se puede observar en la Figura 2, los tres *frameworks* coinciden en que la evaluación del contexto organizacional es el primer paso clave en la gestión de riesgos. Así mismo, concluyen que hay varios aspectos que se deben tener en cuenta en esta actividad y que se relacionan con la gobernanza de Tecnologías de Información, que proviene de la planeación estratégica organizacional como lo son la planeación, el direccionamiento estratégico, las capacidades y servicios de las TIC. Otro factor clave tiene que ver con el factor humano y con los riesgos que provienen de la utilización e incorporación de las TIC en el negocio.

A pesar de la claridad que ofrecen estas guías para definir lo qué es necesario hacer en términos de la evaluación del contexto organizacional, poco se ofrece en torno a cómo se debe empezar a realizar esta evaluación en el día a día de la empresa.

Ahora bien, teniendo en cuenta que la mayor parte de la evaluación del contexto organizacional está relacionada con la gobernanza de TIC, la primera propuesta que se presenta en este artículo es implementar la evaluación utilizando los procesos catalizadores de COBIT (*Control Objectives for Information and related Technology*). El marco de referencia de COBIT 5.0 introduce 37 procesos catalizadores, los cuales se constituyen en una guía para evaluar y diagnosticar el estado actual de la integración de las TIC en la organización en términos de su gestión [27] [28].

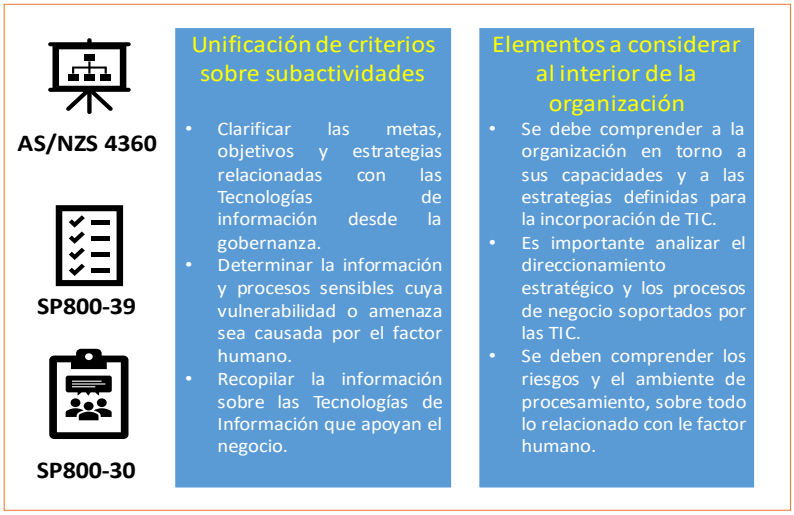

Figura 2. Revisión de guías que relacionan la evaluación del contexto organizacional. Fuente: Elaboración propia.

3.1. Indicadores para su evaluación

Con base en los procesos definidos por COBIT, se diseñó un primer instrumento para la evaluación del contexto organizacional. El instrumento cuenta con un total de 24 preguntas con cuatro posibilidades de respuesta, enmarcadas en los niveles de madurez de los procesos catalizadores (ver Tablas 1 y 2) y relacionadas con los criterios de las guías AS/NZS, SP800-30 y SP800-39.

Las 24 preguntas se agruparon en seis dominios, sobre los cuales se establecerán los diferentes análisis del contexto organizacional para la incorporación de TIC en el negocio: plan estratégico, inversiones, procesos, direccionamiento estratégico, personal, desempeño y capacidad y entrega de servicios TIC.

Los niveles de madurez se agruparon en cuatro a saber: proceso incompleto, proceso ejecutado, proceso establecido / predecible y proceso optimizado. Cada uno de ellos se refleja en las opciones de respuesta de las preguntas del instrumento, lo cual permite una cohesión con los resultados de este.

Tabla 1. Alineación de la estrategia propuesta con los procesos catalizadores de COBIT.

Dominio	Pregunta del instrumento	Alineación con COBIT
Plan estratégico de TIC	¿La administración tiene claramente definido un plan estratégico de Tecnología de Información y Comunicación? ¿En el plan estratégico de TIC se encuentra definida la distribución de los recursos financieros? ¿El plan estratégico ha definido metas e indicadores de evaluación de los proyectos de TIC? ¿Se han efectuado evaluaciones a los planes estratégicos de TIC?	EDM01, APO01, APO02
Inversiones en TIC	¿Existe un plan para la adquisición o restructuración de TIC? ¿Se han definido procesos para informar al personal relevante sobre la adquisición e implementación de las TIC? ¿Al momento de adquirir TIC o desarrollarlas, se aplican estándares para su aprobación? ¿Los proyectos de TIC están vinculados al portafolio de proyectos de la organización?	APO03 BAI01, BAI03

Dominio	Pregunta del instrumento	Alineación con COBIT
Procesos de Tecnología de Información y Comunicación	¿Existe un marco de trabajo para los procesos relacionados con TIC? ¿Se realiza un seguimiento a los cronogramas de actividades de los proyectos TIC? ¿Se han definido, planeado e implantado mediciones para monitorear el cumplimiento continuo del sistema de administración de la calidad de los servicios relacionados con las TIC? ¿Se han asignado prioridades y planeado las actividades identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución de control en todos los niveles para implantar las respuestas a los riesgos asociados a las TIC? ¿Se documentan los inconvenientes evidenciados en la ejecución de cada uno de los proyectos TIC?	APO04, APO05, DSS03
Direccionamiento Estratégico	¿La organización ha establecido un comité encargado del direccionamiento y asesoramiento de la incorporación de las TIC a los procesos de negocio? ¿Se han definido roles y responsabilidades de los actores relacionados con las TIC? ¿Se han definido e implantado políticas y procedimientos para controlar las actividades de los consultores y otro personal contratado por la función de TI ? ¿Se administran y controlan los riesgos relacionados con TIC, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento?	EDM03, APO09
Personal de TIC	¿Se han realizado sesiones de capacitación de forma regular respecto a los procesos, los roles y las responsabilidades de los actores de las TIC en caso de riesgo? ¿La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implantar y monitorear planes de seguridad de TIC? ¿Se realiza una adecuada transferencia de conocimiento a la gerencia?	APO07, APO08, BAI08
Desempeño, capacidad y entrega de servicios TIC	¿Se toman medidas cuando el desempeño y la capacidad de las TIC no están en el nivel requerido? ¿Se ha definido y administrado una estrategia de distribución para asegurar que los planes de contingencia ante riesgos se distribuyan de manera apropiada y segura? ¿Se han determinado todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa? En caso de actualizaciones a sistemas existentes, ¿se realiza un análisis de impacto, justificación costo/beneficio y administración de requerimientos?	EDM05, APO12, APO13, BAI04, BAI06, DSS04

Fuente: Elaboración propia

Tabla 2. Niveles de madurez definidos.

Nivel	Descripción General
Nivel 0. Proceso incompleto	El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.
Nivel 1. Ejecutado	El proceso implementado alcanza su propósito, pero éste se desarrolla de manera ad hoc.
Nivel 2. Establecido/Predecible	El proceso está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
Nivel 3. Optimizado	El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas empresariales presentes y futuros.

Fuente: Elaboración propia.

Tabla 3. Relación de las preguntas con los niveles de madurez.

Nivel	Dominio Personal TIC
Nivel 0. Proceso incompleto	Existe un plan para la adquisición o restructuración de TIC
Nivel 1. Ejecutado	Se han definido procesos para informar al personal relevante sobre la adquisición e implementación de las TIC
Nivel 2. Establecido/Predecible	Al momento de adquirir TIC o desarrollarlas, se aplican estándares para su aprobación.
Nivel 3. Optimizado	Los proyectos de TIC están vinculados al portafolio de proyectos de la organización.

Fuente: Elaboración propia.

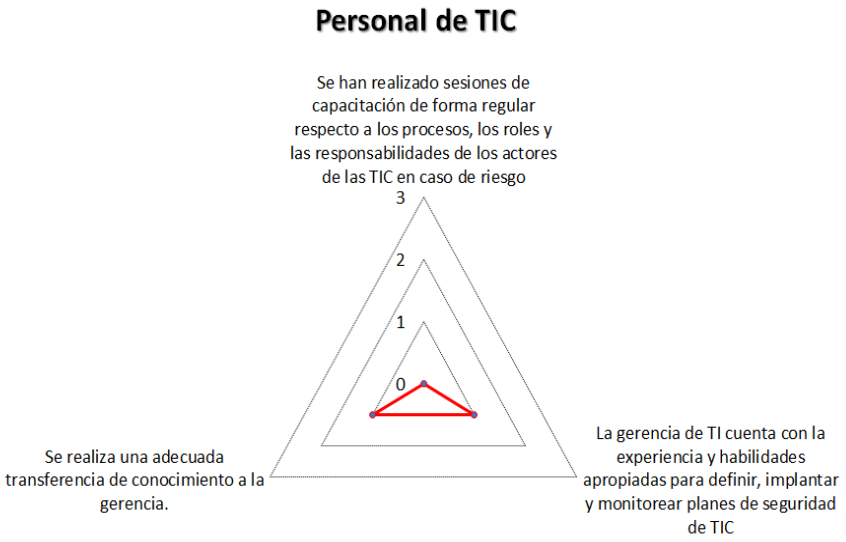

Figura 3. Ejemplo de gráfico de nivel de madurez con base en el modelo. Fuente: Elaboración propia.

A continuación, se presenta un ejemplo del gráfico de resultados, el cual permite relacionar cada una de las preguntas por aspecto evaluado, mostrando el nivel de madurez en cada una de ellas (ver Figura 3). La forma correcta de leer la gráfica está relacionada con los niveles presentados en la Tabla 2. Para el caso, personal de TIC, es evaluado con cuatro opciones de respuesta que están relacionadas con los niveles de madurez como se evidencia en la Tabla 3.

En la Figura 3 se puede observar que la empresa evaluada tiene aspectos imperativos que mejorar en torno al sistema de capacitaciones del personal con respecto a riesgos asociados con las tecnologías que manejan, con una alta probabilidad de que los casos que se presenten únicamente puedan ser solucionados por el jefe de tecnología. No obstante, un aspecto positivo encontrado tiene que ver con la transferencia de conocimiento a la gerencia, en donde se evidencia que existe una biblioteca formal en donde se guarda la documentación sobre privilegios, segregación de tareas, controles automatizados, respaldo/recuperación, seguridad física y riesgos y esta puede ser accedida por la gerencia en caso de ser necesario.

Recapitulando sobre los elementos clave en la evaluación del contexto organizacional, el siguiente tema que se debe tener en cuenta es el relacionado con el factor humano y con los riesgos que provienen de la utilización e incorporación de las TIC en el negocio. Por ello, en la investigación realizada se propuso un instrumento que permitirá diagnosticar las amenazas y vulnerabilidades a las cuales se encuentra expuesta la organización y cuya fuente puede relacionarse con los actores responsables o involucrados con las TIC. Para el diseño de esta herramienta se diseñaron 30 preguntas distribuidas en dos aspectos: "lo que compete a los actores" y "lo que compete a la dirección de TIC", esto basándose en los postulados publicados por [29] en donde se discutió sobre los procesos de cambio que debían darse en la cultura organizacional para que se incorporara la necesidad de cambiar y de aplicar las medidas establecidas para la gestión del riesgo. Algunas de las preguntas planteadas y sus opciones de respuesta se presentan en la Tabla 4.

Tabla 4. Instrumento para el análisis de amenazas y vulnerabilidades.

"Lo que compete a los actores"	**"Lo que compete a la dirección de TIC"**
¿Cuál es la estrategia utilizada por la empresa para mantener actualizados sus sistemas informáticos? a. Se delega esta responsabilidad a cada usuario de equipo y esto se realiza cada que se puede. b. Se delega esta responsabilidad al jefe de TI o auxiliar de soporte técnico. c. Se subcontrata el mantenimiento técnico informático.	¿Ha realizado capacitaciones o entrenamientos en el área de la ciberseguridad? a. No y considero que no son necesarias en la empresa. b. Considero que son necesarias pero no se han realizado. c. Se han realizado esporádicamente pero no hacen parte de un plan.
¿Cuáles son los sistemas de protección utilizados en sus equipos informáticos? a. No conozco cuáles son. b. Conozco cuáles son pero no se para que sirve cada uno de ellos. c. Conozco cuáles son y su utilidad.	¿La empresa ha definido una política de Ciberseguridad? a. No existe una política claramente definida. b. Existe una política pero no es conocida por todos los empleados. c. Existe una política y esta es apropiada por todos los empleados, se evalúa constantemente.
¿Conoce usted la política de protección de datos personales de la empresa? a. La empresa no tiene una política de protección de datos personales. b. Conozco la política pero la aplico sólo para los clientes y proveedores. c. Aplico la política en el marco de lo establecido por la empresa.	¿La empresa ha definido alguna política para gestionar las contraseñas de los sistemas informáticos? a. No, cada usuario gestiona sus propias contraseñas. b. Si, las contraseñas son otorgadas por la empresa o son escogidas por los usuarios siguiendo un patrón definido por la empresa. c. Existe una política clara de gestión de contraseñas, con protocolos de modificación y diseño.
¿Cuándo tiene que salir de su oficina como es su actuación con la sesión del computador? a. Acostumbro a dejar la sesión abierta. No me preocupo por ello.	¿Su personal cuenta con conocimientos específicos en el tema de Ciberseguridad? a. No o no estoy seguro b. Sí, pero son conocimientos básicos

"Lo que compete a los actores"	"Lo que compete a la dirección de TIC"
b. Cierro la sesión sólo cuando me voy a demorar por fuera de la oficina. c. Siempre que me levanto de mi puesto de trabajo cierro la sesión de mi computador.	c. El personal ha recibido diversas capacitaciones y entrenamientos en esta área y se ha comprobado su apropiación.

Fuente: Elaboración propia.

4. Ejemplificando la propuesta

Con el fin de evidenciar la aplicabilidad de las estrategias definidas en la investigación y presentadas en este artículo, se puso en marcha su aplicación en una empresa del sector de servicios de software, la cual enfatiza su actividad principal en la creación de sistemas del sector eléctrico con un alto posicionamiento a nivel nacional en Colombia. Por efectos de confidencialidad, sólo se presentarán algunos de los hallazgos en términos de amenazas y vulnerabilidades.

4.1. Plan estratégico TIC

Dentro de las fortalezas detectadas se encontró que la empresa define un plan estratégico de TIC, al igual que sus procesos. No obstante, no está asociado con la estrategia organizacional, no se han incorporado indicadores y se desconocen los recursos financieros asociados a la inversión o gasto (ver Figura 4).

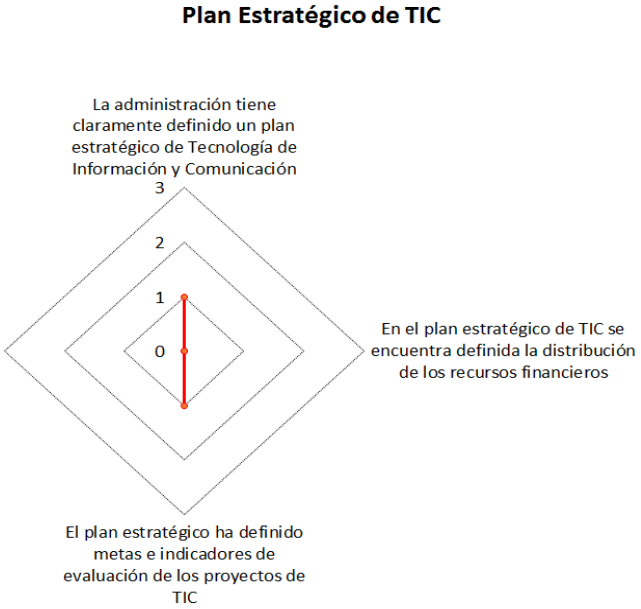

Figura 4. Resultados de los niveles de madurez asociados con el plan estratégico. Fuente: elaboración propia.

Aunque la empresa cuenta con un plan estratégico de tecnología, este no está bien definido pues no contempla todos los elementos que permitan medir la funcionalidad y uso de recursos de las inversiones que se realizan. Lo anterior según Aguilera [30], cobra relevancia si se tiene en cuenta que para ser más competitivos se debe girar en torno a un alineamiento estratégico de las TIC con el negocio.

4.2. Inversiones en TIC

Con respecto a las inversiones en tecnología, la empresa no tiene definido un plan para esta actividad y tampoco realiza seguimiento y control sobre las inversiones. Aunque tiene en cuenta al personal relevante cuando se va invertir en algún tipo de tecnología para el negocio, éste sólo se informa después de la adquisición o a través de

necesidades puntuales. Así mismo, la empresa no ha definido estándares para la aprobación de la adquisición o desarrollo de las TIC y normalmente los sistemas son desarrollados o adquiridos por la familiaridad del jefe de TIC o por recomendaciones de proveedores.

De acuerdo con los resultados, la falta de seguimiento y control es evidente y esto implica según [31], que no se posibilita el aprendizaje organizacional ni la adecuada toma de decisiones. La mayoría de las inversiones se hace por decisiones individuales o recomendaciones externas que no han sido previa y pertinentemente evaluadas. A pesar de que se realizan proyectos de tecnología, las evaluaciones sobre los mismos son informales y no se gestiona el conocimiento sobre las fallas y la ejecución.

4..3 Procesos TIC

En el marco de los procesos de tecnología, las responsabilidades, las relaciones con terceros y funciones han sido claramente definidos y están basados en buenas prácticas. Sin embargo, el cumplimiento de los tiempos en la ejecución de proyectos se deja a cada gerente de proyecto. Así mismo, se realizan evaluaciones informales sobre los riesgos y se suele aplicar sólo a nivel de la alta dirección. Un aspecto importante que se observó débil en el plan estratégico de la empresa, es que no se tiene en cuenta cómo impacta la mala ejecución de un proyecto y/o sus fallas al negocio.

4.4. Direccionamiento estratégico TIC

La organización ha definido un comité que administra y controla la aplicación de las TIC a los procesos de negocio, pero la asignación de los roles y las responsabilidades de los actores relacionados con TIC se realiza dependiendo de las necesidades momentáneas de la empresa. Un aspecto por mejorar es que, aunque se dispone de contratos para controlar las actividades de los consultores y otro personal contratado por la función de TI, el control es informal y la protección se realiza de manera reactiva.

4.5. Personal TIC

Con respecto al personal, la empresa no ha realizado capacitaciones en temas de gestión de riesgos. Cuando suceden casos de riesgo se solucionan por parte del encargado de TIC. Se cuenta con personal capacitado en diferentes aspectos de sus funciones en la organización, como una fortaleza de la empresa, pero no se está sacando el provecho suficiente de ello. No se propende por un enfoque proactivo sino reactivo ante las responsabilidades relacionadas con las TIC [32].

4.6. Desempeño, capacidad y entrega de servicios TIC

Se llevan a cabo algunas medidas cuando el desempeño y la capacidad de las TIC no están en el nivel requerido, pero toma mucho tiempo diagnosticar y solucionar. Las respuestas de los usuarios están centradas en la interrupción. No existe un plan de continuidad documentado, se toman medidas reactivas con frecuencia llevadas a cabo por el mismo usuario, ver Figura 5.

La continuidad del servicio no es gestionada por la organización, colocando en riesgo la comercialización que se realiza a través de herramientas tecnológicas. Este aspecto es de sumo cuidado, toda vez que los costos de recuperación pueden ser más altos que los de protección que no han sido analizados [33].

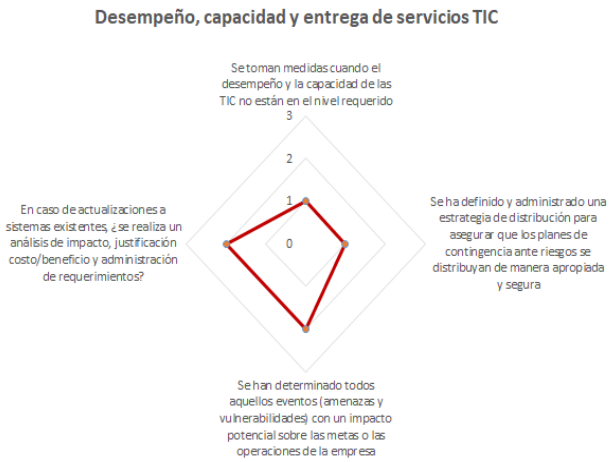

Figura 5. Resultados de los niveles de madurez asociados con el desempeño, la capacidad y la entrega de servicios. Fuente: elaboración propia.

4.7. Análisis de amenazas y vulnerabilidades

Teniendo en cuenta que las amenazas y vulnerabilidades a nivel de TIC en una empresa se constituyen en información confidencial [34], en este artículo se presentaran algunos aspectos generales de los hallazgos encontrados con la estrategia definida para la evaluación del contexto organizacional, más no se profundizará en criterios particulares de la empresa analizada.

Uno de los primeros elementos importantes que arroja el instrumento es la posibilidad de contrastar dos posiciones a nivel empresarial. Por un lado, lo que los actores que utilizan diariamente la tecnología piensan y ejecutan a nivel de manejo de riesgos; y otra, lo que quienes administran y definen las políticas piensan que se está haciendo en la empresa. Por ejemplo, para el caso de la empresa cuyos resultados se muestran en este artículo, se pudo corroborar que más del 80% de los empleados maneja las políticas de riesgos y conoce las estrategias que se utilizan por ejemplo para mantener actualizados sus sistemas informáticos o para modificar sus contraseñas, sin embargo, hay otro porcentaje restante que desconoce totalmente el tema y que de hecho manifiesta que se maneja de manera externa.

Así mismo, se pudo evidenciar que, aunque la dirección tecnológica ha implementado sistemas de protección en todos los equipos de la empresa, un porcentaje importante de empleados (más del 70%), no sabe para que se utilizan o no sabe cuáles son (ver Figura 6). Este resultado se repite en criticidad en lo concerniente con la política de manejo de desechos de información y dispositivos con información de la empresa, ya que un preocupante 84% de los empleados no la aplica o simplemente la desconoce.

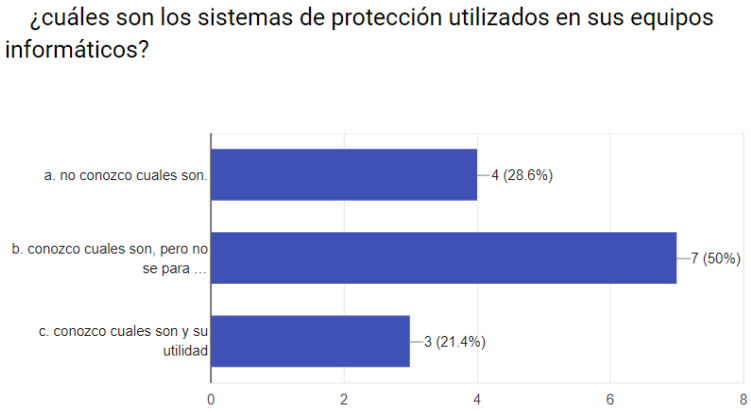

Figura 6. Ejemplo de los resultados de la evaluación. Fuente: elaboración propia.

La mayoría de los empleados en la empresa no están capacitados para actuar ante un ataque de seguridad de la información y esto incluso es evidenciado por la dirección tecnológica, quien en concordancia con los hallazgos reconoce a partir de la aplicación del modelo propuesto que se ha descuidado este tema en la empresa y que las amenazas a las cuales puede estar expuesta debido a ello son cada vez más altas. Con base en los resultados de la aplicación del modelo, algunas de las amenazas y vulnerabilidades detectadas se presentan en la Tabla 5.

Como se pudo observar, el proceso de validación del modelo propuesto, abordado no sólo con la empresa cuyos resultados se presentaron, sino con otras de diferentes sectores económicos, permite obtener una "mirada" del contexto organizacional en materia de la gestión de riesgos en tecnologías de información y comunicación. Es importante resaltar que este es sólo el primer paso de un modelo más grande para la gestión de riesgos que posteriormente permita definir escenarios de riesgo y controles para mitigarlos.

Tabla 5. Amenazas y vulnerabilidades identificadas en la empresa.

Amenazas	Vulnerabilidades
• Fuga de información. • Intrusión de software malicioso. • Acceso no autorizado. • Robo y pérdida de información. • Falla en la continuidad del servicio. • Espionaje industrial.	• Los empleados • Desconocen las políticas de seguridad. • Revelan información confidencial. • No protegen sus documentos y sesiones de trabajo. • No están capacitados. • La dirección de TI • No capacita a los empleados. • No asegura los niveles de servicio. • No realiza seguimiento a la aplicación de las políticas.

Fuente: elaboración propia.

5. Conclusiones

El crecimiento acelerado de las tecnologías tiene todavía muchos aspectos que deben ser abordados desde una perspectiva de gestión del riesgo, es por ello que las organizaciones deben ser mesuradas al momento de implementarlas, toda vez que al ser parte de un sistema complejo que es la empresa, cualquier error puede generar un caos, desdibujando el propósito y los beneficios que puede aportar.

Las estrategias propuestas en este artículo se apoyan en una de las primeras actividades definidas para la gestión de riesgos por varios marcos de referencia internacionales y que está relacionada con el establecimiento del contexto organizacional. El establecimiento del contexto organizacional para la alineación de las Tecnologías de la Información con su direccionamiento estratégico requiere de instrumentos que permitan obtener un panorama completo de lo que la empresa ha dispuesto a nivel directivo, estratégico y operacional para una adecuada incorporación de las TIC.

Un adecuado diagnóstico de las amenazas y vulnerabilidades a las cuales se encuentra expuesta la empresa y cuya fuente puede relacionarse con los actores de las TIC, implica propuestas innovadoras como la presentada en este artículo en las que se evalúen no sólo desde lo que es responsabilidad de la empresa sino también desde la responsabilidad misma de dichos actores TIC. Un aspecto importante que destacar, después de la aplicación de la propuesta presentada en este artículo es que la simplicidad de su puesta en marcha permite que pueda ser aplicado sin mayor dificultad y que la correlación con los niveles de madurez se haga rápidamente sin perder el rigor en la presentación de los resultados.

6. Agradecimientos

Este artículo es uno de los resultados del proyecto doctoral "Modelo para la gestión de riesgos en TIC, desde el enfoque de las organizaciones inteligentes" realizado con apoyo de la Universidad Internacional Iberoamericana de México y la universidad de Santander UDES.

7. Referencias

[1] Palacios, L. (2016). *Dirección estratégica*. España: Ecoe Ediciones.

[2] Briceño Zamudio, M. C., Martínez Moreno, E. T. (2015). *Direccionamiento estratégico. Evolución y estado del arte*. México: Ediciones EAE.

[3] Kalkan, A., Çetinkay, Ö., Arman, M. (2014). The Impacts of Intellectual Capital, Innovation and Organizational Strategy on Firm Performance. *Procedia - Social and Behavioral Sciences,* 150 (15), 700-707.

[4] FlySteensen, E. (2014). Five types of organizational strategy. *Scandinavian Journal of Management*, 30 (3), 266-281.

[5] García-Peñalvo, F. J. (2018). *Gobierno de Tecnologías de la Información*. (1era ed.) [versión electrónica] Recuperado de: http://repositorio.grial.eu/handle/grial/1229

[6] Suárez Marrufo, M. C., Salinas Mendoza, B. (2014). Uso de las tecnologías de información y comunicación en la apropiación social del conocimiento como base para el desarrollo de estrategias de gestión en ciencia y tecnología. *Revista de Investigación en Tecnologías de la Información*, 2 (4), 14-20.

[7] ISO/IEC (2015). *Corporate governance of information technology*, ISO/IEC 38500.

[8] Muñoz, I., Ulloa, G. (2011). Gobierno de TI – Estado del arte. *Revista Sistemas & Telemática*, 9 (17), 23-53.

[9] Díaz, H. (2017). Tecnologías de la información y comunicación y crecimiento económico. *Revista Economía Informa,* 405, 30-45.

[10] Guerrero, M. (2017). Una aproximación a la gestión de riesgos y controles en tecnologías de información desde la perspectiva desde las organizaciones inteligentes. *Revista Nousitz*, 1 (1), 33-39.

[11] Valencia-Duque, F. J., Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, 22, 73-88. doi: http://dx.doi.org/10.17013/risti.22.73-88.

[12] Guerrero, M., Gómez, L. (2012). Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional. *Revista Estudios gerenciales,* 28 (125), 87-95.

[13] Isaca (2012). *Risk IT Framework for Management of IT Related Business Risks.* Urs Fischer, CISA, CRISC ISACA Guidance and Practices Committee.

[14] Caralli, R., Stevens, J., Young, L., Wilson, W. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Software Engineering Institute*. CMU/SEI Report Number: CMU/SEI-2007-TR-012.

[15] Lydon, B. (2016). *Industry 4.0: Intelligent and flexible production* [versión electrónica] Recuperado de: http://www.isa.org

[16] Zhou, K., Liu, T. (2015). Industry 4.0: Towards Future Industrial Opportunities and Challenges. *Presentado en 12th International Conference on Fuzzy Systems and Knowledge Discovery*, Changsha, China.

[17] Fojon, E., Sanz, A. (2010*). Ciberseguridad en España. Una propuesta para su gestión* [versión electrónica]. Recuperado de: http://biblioteca.ribei.org/1879/1/ARI-102-2010.pdf

[18] Hernández Moreno, A. (2017). Ciberseguridad y confianza en el ámbito digital. *Información Comercial Española, ICE: Revista de economía*, (897), 55-65.

[19] Ernst & Young. (2016*). Cambios en el panorama de los riesgos de TI. El porqué y el cómo de la actual Administración de Riesgos de TI*. [versión electrónica] Recuperado de: http://www.ey.com/Publication/vwLUAssets/Cambios_en_el_panorama_de_los_riesgos_de_TI/$FILE/Perspectivas_riesgos_TI.pdf

[20] Cisco (2018). *Informe de Ciberseguridad anual*. Estados Unidos: Cisco.

[21] Carpentier, J. F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas*. Barcelona: Ediciones ENI.

[22] Guerrero, M., Gómez, L. (2011). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en sistemas de información. *Revista Estudios gerenciales,* 27 (121), 195-218.
[23] Ramírez, A., Ortiz, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Revista Ingeniería*, 16 (2), 56-66.
[24] 4360:2004 (2004). *Estándar Australiano. Administración de Riesgos*. Tercera edición. Australia: Standards.
[25] Stonebumer, G. (2002). *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology*. NIST. Estados Unidos: Special Publication 800-30.
[26] Ross, R. (2008). *Managing Risk from Information Systems. Recommendations of the National Institute of Standards and Technology*. Gaithersburg: NIST Special Publication 800-39.
[27] Isaca (2012). *COBIT 5.0. Enabling Processes*. Estados Unidos: Isaca.
[28] Isaca (2012). *COBIT 5.0. Un marco de negocio para el gobierno y la gestión de TI de la empresa*. Estados Unidos: Isaca.
[29] Guerrero, M. (2015). Descifrando los procesos de cambio de la cultura organizacional para la gestión de riesgos y controles en sistemas de información. *Revista Nousitz*, 1 (1), 797-802.
[30] Aguilera, A., Riascos, S. (2009). Direccionamiento estratégico apoyado En las TIC. *Revista Estudios Gerenciales*, 25 (111), 127-143.
[31] López, D. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. *Revista Tecnológica ESPOL*, 30 (1), 51-69.
[32] Hinarejos, A., De la Peña, J. (2017). I+D+i y ciberseguridad análisis de una relación de interdependencia. *Revista Cuadernos de estrategia,* 185, 247-290.
[33] Ramírez, A., Ortiz, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Revista Ingeniería*, 16 (2), 56-66.
[34] Santiago, E., Sánchez, J. (2017). Riesgos de ciberseguridad en las Empresas. *Revista Tecnología y desarrollo*, 15, 1- 33.