

# ANÁLISIS DE LA GESTIÓN DE RIESGOS EN LAS UNIDADES DE TECNOLOGÍA DE LA INFORMACIÓN DE LAS INSTITUCIONES PÚBLICAS DE MANABÍ-ECUADOR

Jorge Luis Mendoza Loor<sup>1</sup>, Junior Antonio Briones Mera<sup>2</sup>, Henry Fabricio Mendoza Cedeño<sup>3</sup>, Kenia Marilú Mendoza Vega<sup>4</sup>

{jorgel.mendoza<sup>1</sup>, junior.briones<sup>2</sup>, henry.mendoza<sup>3</sup>, kenia.mendoza<sup>4</sup>}@uleam.edu.ec

ORCID: <https://orcid.org/0000-0002-0150-787X><sup>1</sup>

Universidad Laica Eloy Alfaro de Manabí Extensión Chone

Recibido (27/09/19), Aceptado (16/10/19)

**Resumen:** Se presenta un análisis de las condiciones de riesgo presentes en las unidades de Tecnología de la Información (TI), donde reposan los datos e información académica de las universidades. En este estudio se ha evaluado al personal de las unidades de TI de diferentes instituciones de la provincia de Manabí en Ecuador. Para ello se han considerado los perfiles académicos, y la participación de los mismos en la gestión de protección de la información. Para la ejecución de este trabajo se han realizado encuestas al personal de TI, con un total de 360 personas encuestadas que componen la muestra. El análisis realizado permitió comprobar los niveles de seguridad y calidad de los servicios de Tecnología de la Información que ofrecen los departamentos de las instituciones evaluadas, a su vez fue posible constatar la gestión de conocimiento presente en las 40 instituciones estudiadas.

**Palabras Claves:** Tecnología de la Información, Gestión de Riesgo, Seguridad Informática, Protección de la Información.

## ANALYSIS OF RISK MANAGEMENT IN INFORMATION TECHNOLOGY UNITS

**Abstract:** An analysis of the risk conditions present in the Information Technology (IT) units is presented, where the academic data and information of the universities rest. In this study the personnel of the IT units of different institutions of the province of Manabí in Ecuador have been evaluated. For this, the academic profiles and their participation in the management of information protection have been considered. For the execution of this work, surveys have been carried out on IT personnel, with a total of 360 people surveyed that make up the sample. The analysis made it possible to verify the levels of security and quality of the Information Technology services offered by the departments of the evaluated institutions, in turn it was possible to verify the knowledge management present in the 40 institutions studied

**Keywords:** Information Technology, Risk Management, Computer Security, Information Protection.

## I. INTRODUCCIÓN

Las nuevas empresas y las nuevas tendencias de negocio hacen que cada vez sea más necesaria la utilidad de las tecnologías de la información (TI), entendiéndose estas como aquellas herramientas que nos conectan con el mundo y permiten la optimización de recursos informáticos, recursos de procesamiento de información y recursos publicitarios. Hay muchos esfuerzos hacia la creación de medios para una gestión exitosa de las TI. Estos esfuerzos incluyen métodos para garantizar el valor de la TI, la gestión de los riesgos relacionados con TI y mayores requisitos de control [1]. Las nuevas tendencias empresariales son cada vez más dependientes de las TI, y ello involucra un conjunto de elementos que impulsan y permiten la gestión empresarial de forma exitosa [2], haciéndose indispensable para el sustento del negocio. Así pues la gestión de TI debe tratarse de forma seria y con mucha responsabilidad, con el fin de garantizar que las TI apoyen totalmente a la gestión empresarial, y no se conviertan en un problema adicional dentro de la administración general de las organizaciones.

Uno de los aspectos considerados para una efectiva gestión de TI es la orientación al cliente [3], de ahí que destaque la relevancia de las TI para una apropiada gestión empresarial, junto con los procesos inherentes al negocio. Considerando las estructuras institucionales, es necesario tomar en cuenta la arquitectura empresarial, entendida así como la organización fundamental de una empresa, ya sea como un todo, o junto con socios, proveedores y/o clientes o en parte, así como los principios que rigen su diseño y evolución [4]. Considerando esta arquitectura es posible definir el tipo de gestión de TI que se debe implementar según el tipo de empresa a desarrollar.

La arquitectura empresarial puede apoyar la alianza entre las TI y el negocio desde un análisis de dependencia, análisis de cobertura, análisis de interfaz, análisis de heterogeneidad, análisis de complejidad, análisis de cumplimiento, análisis de costo y beneficio [4]. Para considerar una gestión integral de TI es necesario tomar en cuenta los aspectos asociados a planificación de continuidad de negocio, gestión de seguridad, gestión de riesgos tecnológicos, planificación de portafolio de proyectos, rediseño de procesos de negocio, gestión de calidad y cumplimiento, integración de post-fusión, introducción de software comercial, decisiones de abastecimiento, administración de TI y de operaciones de TI, así como consolidación de TI.

Las nuevas tecnologías de la información y la comunicación (TIC), crean y respaldan los sistemas de información que se integran con personas y procesos para

proporcionar servicios de negocios y gubernamentales [5]. Las organizaciones ofrecen servicios de tecnologías de la información y comunicación, están en constantes presiones laborales para asegurar la calidad de los servicios y ofrecer estabilidad en las herramientas que se requiere para los usuarios. Algunos autores [6] aseguran que un importante número de empresas del Ecuador no tienen un modelo de operación de los servicios de tecnología basado en las mejores prácticas que esté orientado a los clientes, esto se refiere al liderazgo, los procesos, el impacto en la sociedad, resultados globales del negocio y la mejora continua, lo cual conduce a un distanciamiento de la mejora continua, de la búsqueda de la excelencia y por ende conduce a las empresas a ser poco competitivas. En el Ecuador no es muy común que las empresas públicas utilicen marcos de trabajo o modelos estandarizados de TI que sean reconocidos internacionalmente. Algunas entidades lo han hecho basadas en sus propias experiencias y en las ideas de los encargados de los departamentos de TI, lo cual hace que sea de alto riesgo las fallas en el negocio, por no poseer la información y documentación apropiadas. Un pequeño grupo de empresas relativamente grandes y especialmente las empresas del sector privado toman este tipo de actividades con la responsabilidad del caso [7].

En el Ecuador existen varias iniciativas aisladas para solventar la gestión de TI, por ejemplo en las referencias [7], [8] han desarrollado propuestas para el sector público del Ecuador y han detectado importantes factores que deben ser mejorados para lograr una gestión eficiente. Así mismo Villacís y William [9] que han propuesto guías de evaluación de la gestión de TI con aplicación de COBIT Y COSO en el sector público ecuatoriano, sin embargo estas propuestas muchas veces no se masifican y terminan por quedar estériles en el tiempo, por lo tanto el problema de la gestión integral de TI se agudiza. Otros autores como Viteri et al [7] han desarrollado estudios en las áreas de TI donde se han evaluado los niveles de desarrollo y de proceso, logrando considerar los factores que destacarían una gestión más óptima. Por otro lado Oviedo et al [10] se ha evaluado la seguridad informática de una unidad de TI y se han propuesto herramientas de software para mejorar la protección de la información en las instituciones estatales. En todos los casos descritos ha habido preocupación por la gestión de TI, pero no se ha considerado la inversión necesaria de tiempo, dinero y recursos humanos para la optimización de las unidades de TI en el Ecuador.

Desde la educación superior, los estudiantes y profesionales de Ingeniería en Sistemas y carreras afines deben conocer de forma clara la realidad en cuanto a los niveles de madurez tecnológica, aplicación de nor-

mas y/o estándares, gestión de riesgos de TI, niveles de Outsourcing, niveles de seguridad, calidad del servicio y la gestión del conocimiento en torno a la gestión integral de TI desarrollada en las instituciones tanto públicas como privadas, priorizando su preparación en el conocimiento de soluciones que permitan mejorar la realidad de las instituciones, con la finalidad de aprovechar de mejor manera los recursos técnicos, operativos, financieros y de tiempo. El objetivo de este trabajo es realizar una investigación in situ para evaluar la gestión de TI y la seguridad informática en las instituciones de la provincia de Manabí, con el fin de conocer la actualización tecnológica de los departamentos de TI y proponer mejorar sustanciales en torno a la optimización de recursos, la actualización de tecnología y la gestión por procesos para la administración y manejo de datos informáticos.

Este trabajo está conformado por tres secciones adicionales a esta; la segunda sección trata sobre los conceptos fundamentales que sustentan esta investigación, en la sección tres está la metodología desarrollada y en la sección cuatro se presentan los resultados. Finalmente se expone la conclusión.

## II. ELEMENTOS DE LA GESTIÓN DE TI

### A. Arquitectura Empresarial.

Las nuevas tendencias de negocio exigen una arquitectura empresarial bien definida, que se entiende como el conjunto de elementos que fundamentan una organización, que comprende además los principios que rigen su diseño y evolución [4]. Por tanto la arquitectura empresarial es un conjunto de directrices que permite garantizar el desempeño y desarrollo armónico de la empresa, enfocados en el negocio sin descuidar la ges-

ción tecnológica.

### B. Gestión de TI.

La arquitectura empresarial y la gestión de TI son dos elementos de negocios que deben ir asociados entre sí. Las herramientas de TI ofrecen un apoyo indiscutible a la gestión empresarial, más aun en los nuevos tiempos donde el impacto de las empresas está asociado a la comunicación globalizada. Para esto es necesario que las compañías se enfoquen las prácticas de optimización de recursos de TI para mantener la actualización de los sistemas y la mejora continua en el personal responsable de estas unidades de tecnología [5].

Las arquitecturas empresariales se llevan a cabo para definir los lineamientos informáticos que estén enfocados en las necesidades y puedan predecir o prever las futuras necesidades de las organizaciones, en función de una toma de decisión acertada enfocada en la generación de bases de datos integrales, aportando en la generación de estándares de desarrollo empresarial, con calidad de servicios internos, además de disponer del recurso humano necesario para las estrategias propuestas.

### C. Estándares internacionales para la efectiva gestión de TI

La norma ISO/IEC 38500 [11] ofrece un estándar internacional para las buenas prácticas del Gobierno de las Tecnologías de la Información (TI). Su característica principal es llevar el gobierno de TI en las instituciones empresariales, considerando seis principios fundamentales y tres procesos básicos.

Los principios que rigen la Norma ISO/IEC 38500 son los que se muestran en la figura 1, en ella se observan los elementos que hacen posible una óptima gestión de TI.

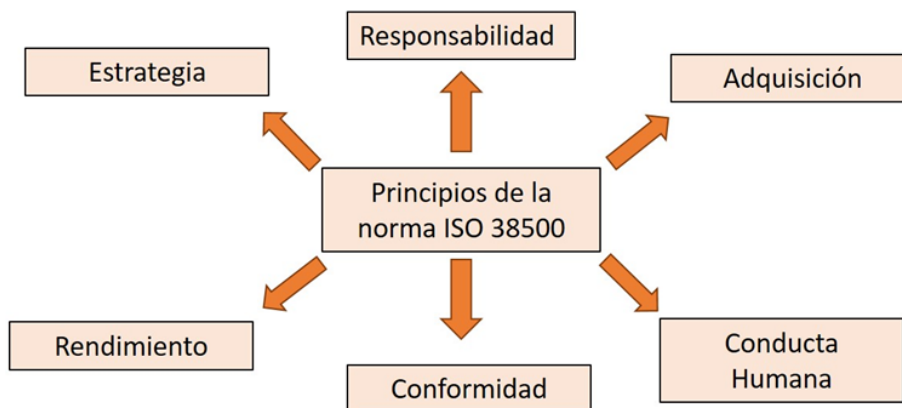
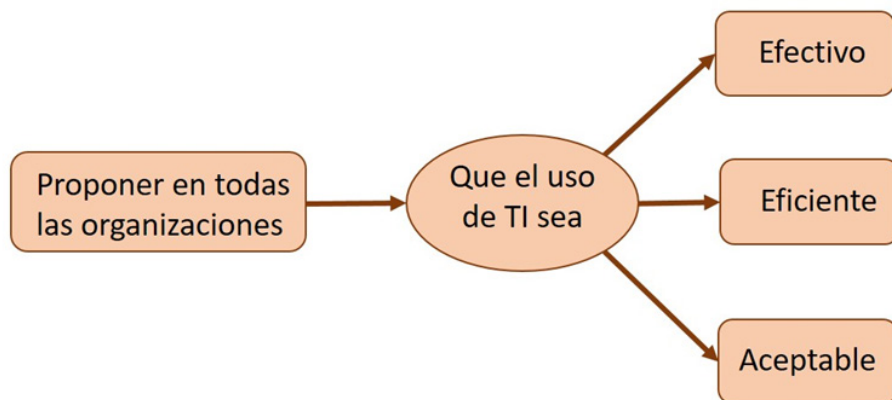


Figura 1. Principios asociados a la norma ISO 38500.

El propósito principal de la Norma ISO 38500 se describe de forma concisa en la figura 2, en ella se pue-

den apreciar los factores que condicionan el objetivo de desarrollar y aplicar esta norma a la gestión empresarial.



**Figura 2. Propósito de la Norma ISO 38500 para las organizaciones.**

Un aspecto fundamental en la gestión de TI es asegurar la calidad, la cual debe ser transversal en todas las actividades de la gestión de TI, por ejemplo, en cuanto a la provisión de servicios de TI, la calidad y el valor de una oferta de servicio pueden evaluarse desde al menos dos perspectivas: la de un proveedor de servicios (la calidad intrínseca del diseño de lo que se ofrece y cómo se gestiona), y la del cliente (la calidad extrínseca de lo que el cliente proporciona y experimenta) [12].

Para evaluar la gestión de TI en las instituciones y organizaciones, es necesario tomar en cuenta el nivel de madurez, que va desde un nivel cero o inexistente hasta un nivel optimizado (5). Estos parámetros permiten caracterizar la gestión de TI de las unidades de tecnologías, y permiten conocer sus debilidades y fortalezas.

### III. METODOLOGÍA

Para este estudio se realizó un método analítico-sintético, donde fue necesario analizar la información existente en la documentación científica para luego plasmarlas en este documento y argumentar lo que aquí se expone.

Además se realizó un método estadístico para el procesamiento de datos y la validación de resultados.

En cuanto a las técnicas realizadas en este trabajo se consideró la evaluación del personal de las unidades de TI, a partir de un conjunto de interrogantes que componen una encuesta. Así mismo estos instrumentos fueron aplicados a los usuarios de TI.

#### A. Sujetos y Tamaño de la Muestra

Este estudio se consideró la evaluación de la gestión de TI en 30 instituciones públicas de la provincia de Manabí, específicamente se consideraron las siguientes unidades de análisis:

Jefes o coordinadores de TI, que corresponde a las personas responsables de los departamentos o áreas de TI dentro de las instituciones involucradas.

Trabajadores de TI, que son los empleados que trabajan en los departamentos de TI.

Usuarios de TI, determinados por las personas que utilizan las TI en las instituciones involucradas.

La población de este estudio estuvo determinada por 4160 personas involucradas en las unidades de análisis mencionadas. Los jefes de TI fueron 40 en total, los trabajadores de TI consistieron en 120 personas, mientras que el restante (4000) corresponde a los usuarios. En vista de que el número de usuarios es abundante, se consideró únicamente un total de 5 usuarios por cada institución evaluada, arrojando un total de 150 personas encuestadas.

### IV. RESULTADOS

Los resultados mostraron que solo el 27% de las personas conoce sobre la gestión de riesgos de tecnología de la información y la importancia de la funcionalidad de esta estructura dentro de la organización. Un 32% de los encuestados refleja tener muy bajos conocimientos al respecto. Y un 27% manifiesta un conocimiento intermedio. Estos resultados reflejan un factor importante para las instituciones, lo cual debería ser considerado para una mejora continua en el proceso de formación profesional, con el fin de asegurar la confiabilidad de los datos y la protección de los mismos. Así mismo es relevante el hecho de que en las instituciones evaluadas existen más personas con responsabilidades de jefes que personas con otro tipo de funciones, por lo que es posible afirmar que un importante número de jefes, aproximadamente 30, no tiene amplios conocimientos en relación a la seguridad informática. Y solo un apro

ximado de 10 jefes conoce ampliamente lo relacionado con la seguridad de la información.

Así mismo, las encuestas revelaron que el 70% de las personas no tiene el suficiente conocimiento con relación a las buenas prácticas de gestión riesgo de TI que deben seguirse para garantizar un funcionamiento óptimo y el resguardo apropiado de la información que se maneja.

En cuanto al conocimiento relacionado con el portafolio de riesgos de tecnología de la información, el 48% afirmó no tener conocimientos al respecto. Lo cual conduce a una necesidad importante de capacitar al personal en torno a estas teorías fundamentales para mejorar el funcionamiento de las unidades de TI en las instituciones públicas.

Por otra parte, el 56% de los encuestados reveló que no se le ha consultado e incluido en las mejoras de la gestión de riesgo, y a su vez estos mismos han sido considerados para participar en la recuperación de la funcionalidad de la infraestructura tecnológica.

El 76% de las personas afirmó que existen algunos mecanismos para implementar la recuperación funcional de la infraestructura tecnológica, sin embargo esto implica que no existen los mecanismos suficientes para mantener la continuidad y la operatividad de las unidades de TI. Estos mecanismos son de vital importancia para las unidades de TI, ya que de ello dependerá la recuperación de la información en caso de desastres, así mismo son necesarios para llevar a cabo una correcta gestión de protección de datos.

Sin embargo, el 32% de las personas evaluadas consideró que la gestión de riesgos realizada es bien definida y se dan a conocer las estrategias, existiendo así una estructura determinada y se evalúan los riesgos tomando en cuenta los parámetros establecidos. También un 32% manifestó que no se hace una completa evaluación de riesgos y que estas a su vez no son las más organizadas ni están completamente definidas. Esto refleja cierta incoherencia en relación al 76% que manifestó no conocer de ciertos mecanismos para el mantenimiento de la información y la recuperación de datos. Estas incongruencias dejan en evidencia la ambigüedad de la información existente en las unidades de TI, lo que representa una situación de interés para las instituciones, las cuales deben asegurar una correcta gestión de TI que mantenga la seguridad de los datos.

## V. CONCLUSIONES

La gestión de riesgos de TI es indispensable para la protección de datos, la continuidad de negocio y la prevención de pérdida de la información.

El uso de la Norma ISO 38500 es de suma impor-

tancia para las instituciones, ya que esto puede asegurar una dirección apropiada de TI, así como la evaluación continua en los procesos y el monitoreo de las actividades, con el fin de implementar proyectos y operaciones que aporten a la mejora continua de la gestión de TI.

Las instituciones deben contar con un gobierno de TI que asegure el cumplimiento de objetivos, que además evalúe las necesidades de los usuarios y de los mismos trabajadores de TI, así como la evaluación de las condiciones de prioridades y de tiempos para los objetivos planteados.

Las instituciones públicas de Manabí no cuentan con una adecuada gestión de riesgos que les permita asegurar los datos en caso de desastres. Además las personas asociadas a las unidades de TI requieren una mayor capacitación para mejorar el aporte que brindan a la gestión de TI; para enriquecer las unidades donde se desempeñan y contribuir de manera óptima a las instituciones.

## REFERENCIAS

- [1]I. Velitchkov, «Integration of IT Strategy and Enterprise Architecture Models,» de Proceedings of the 9th International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing, , New York, 2008.
- [2]E. Kozlova, U. Hasenkamp y E. Kopanakis, «Use of IT Best Practices for Non-IT Services,» de Annual SRII Global Conference, 2012.
- [3]A. Hochstein, R. Zarnekow y W. Brenner, «ITIL as common practice reference model for IT service management: formal assessment and implications for practice,» IEEE, pp. 704-710, 2005.
- [4]C. Braun y R. Winter, «Integration of IT Service Management into Enterprise Architecture,» de Proceedings of the 2007 ACM Symposium on Applied Computing, New York, 2007.
- [5]S. Galup, J. J. Quan, R. Dattero y S. Conger, «Information Technology Service Management: An Emerging Area for Academic Research and Pedagogical Development,» de Conference on Computer Personnel Research: The Global Information Technology Workforce, New York, 2007 .
- [6]R. Bonilla, S. Carolina, Z. Rendón y A. Dolores, «Propuesta de procesos para la fase de operación de los servicios de tecnología fundamentado en ITIL, para Bio Agencia de Comunicación,» 2014.
- [7]Y. Viteri, M. Cano, A. Zambrano y C. Minaya, «Evaluación de las incidencias y riesgos presentes en la infraestructura tecnológica de la Universidad Layca Eloy Alfaro de MANabí-Ecuador,» Revista Universidad, Ciencia y Tecnología, vol. 23, n° 94, 2019.



- [8]N. Ávalos, H. Fabricio, E. Navia y J. Francisco, «Propuesta de gestión tecnológica para la defensoría pública del Ecuador alineada al marco regulatorio del sector público,» Ecuador, 2015.
- [9]V. López y W. Napoléon, «Guía de evaluación de la gestión de TI con aplicación de COBIT Y COSO en el sector público ecuatoriano,» Ecuador, 2014.
- [10]B. Oviedo, E. Shuma y A. Gracia, «Análisis de herramientas de códigos abiertos que permitan la seguridad de la data en las universidad técnica estatal de Quedo,» Revista Universidad, Ciencia y Tecnología, vol. 23, n° 94, 2019.
- [11]coding, «coding or not,» 2018. [En línea]. Available: <https://codingornot.com/gobierno-de-ti-que-es-la-isoiec-38500-y-para-que-sirve>.
- [12]M. Lepmets, A. Cater-Steel, F. Gacenga y E. Ras, «Extending the IT service quality measurement framework through a systematic literature review,» J. Serv. Sci. Res, vol. 4, n° 1, pp. 7-47, 2012.