

TLATEMOANI
Revista Académica de Investigación
Editada por Eumed.net
No. 33 – Abril 2020.
España
ISSN: 19899300
revista.tlatemoani@uaslp.mx

Fecha de recepción: 13 de enero de 2020
Fecha de aceptación: 29 de abril de 2020

PROCEDIMIENTO PARA DIAGNOSTICAR LA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN EMPRESAS

AUTORES:

Diana Ibet Arias Herrera*

dianaibet@nauta.cu

Islay Milián Nieblas**

isy81@gmail.com

Jorge Félix Domínguez Hernández***

jorgefelix@uniss.edu.cu

*Universidad de Sancti Spíritus “José Martí Pérez”. Cuba.

**Tienda Ross Florida EEUU.USA.

***Universidad de Sancti Spíritus “José Martí Pérez”. Cuba.

Centro Universitario Municipal Trinidad, UNISS, Cuba.

RESUMEN

En la investigación se realiza la propuesta de un procedimiento para diagnosticar la gestión de las TI en las empresas, a partir de los objetivos de negocio y la administración de los riesgos, el cual se sustenta teóricamente en los estándares y marcos de trabajo: ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27005:2008, ISO/IEC 38500: 2008,

Jones, Jack A. (2015), asimismo se utiliza el indicador nivel de la gestión de tecnologías de la información (IGTI) basado en el modelo COBIT (Objetivos de Control para Tecnología de Información) y la evaluación de madurez de procesos de las TI en la organización. Se aplican encuestas, entrevistas, revisión de documentos, análisis comparativos y observación. En el procesamiento computacional de los datos el SPSS y el Microsoft Excel. El procedimiento propuesto constituye una herramienta factible para diagnosticar la gestión de las TI en las empresas.

PALABRAS CLAVE: procedimiento, diagnóstico, tecnologías de la información, empresas.

ABSTRACT

PROCEDURE TO DIAGNOSE THE MANAGEMENT OF INFORMATION TECHNOLOGIES IN COMPANIES.

The investigation proposes a procedure to diagnose the management of IT in companies, based on business objectives and risk management, which is theoretically based on the standards and frameworks of work: ISO / IEC 27001: 2005, ISO / IEC 27002: 2005, ISO / IEC 27005: 2008, ISO / IEC 38500: 2008, Jones, Jack A. (2015), the level indicator of information technology management is also used (IGTI) based on the COBIT model (Control Objectives for Information Technology) and the maturity assessment of IT processes in the organization. Surveys, interviews, document review, comparative analysis and observation are applied. In the computational processing of the data the SPSS and the Microsoft Excel. The proposed procedure is a feasible tool to diagnose the management of IT in companies.

KEYWORDS: procedure, diagnosis, information technologies, companies

INTRODUCCIÓN

Las Tecnologías de la Información no son un simple recurso para apoyar las operaciones cotidianas, el uso inteligente de las mismas puede alterar de manera significativa la posición estratégica a largo plazo de una organización en el mercado mundial. La aplicación de los sistemas de información en la planeación, modifica por completo el modo en que una empresa realiza sus actividades. El uso correcto de las TI en una entidad proporciona una adecuada gestión de la calidad, aumento de la eficiencia y alineación de los procesos de negocio y la infraestructura.

Los estudios realizados de las prácticas de gestión de TI en compañías nacionales e internacionales, revelan la escasa optimización de los recursos e inversiones de las mismas. Las empresas cubanas en el transcurso de los años se han insertado en el manejo de estas, pero aún es pobre la gestión de estos recursos y son víctimas del retorno de la inversión y su efectiva explotación en función de los objetivos de negocio. En muchas ocasiones la dirección de la entidad no cuenta con herramientas que le permiten medir el nivel de gestión de las TI, para evaluar los riesgos y beneficios, identificar las oportunidades de mejoras y evaluar su impacto en el logro de los objetivos empresariales.

El objetivo del presente estudio radica en la propuesta de un procedimiento para diagnosticar la gestión de las Tecnologías de la Información en las empresas.

DESARROLLO

La gestión de las TI es utilizar y adaptar las tecnologías de forma que aporten un valor real medible a la estrategia y táctica del negocio. Gestionar las TI, es tomar las decisiones estratégicas y tácticas para aportar valor que genere beneficio. Se asume el criterio del modelo COBIT donde plantea: las Tecnologías de la Información han podido conceptuar como la integración y convergencia de la computación microelectrónica, las telecomunicaciones y la técnica para el procesamiento de datos, sus principales componentes son: el factor humano, los contenidos de la información, el equipamiento, la infraestructura material, el software y los mecanismos de intercambio electrónico de información, los elementos de política y regulaciones y los recursos financieros[ISACA. (2007)].

METODOLOGÍA

Se realizó la consulta bibliográfica de los estándares utilizados en la gestión de las Tecnologías de la Información: ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27005:2008, ISO/IEC 38500: 2008, Jones, Jack A. (2015), se utiliza el indicador nivel de la gestión de tecnologías de la información (IGTI) basado en el modelo COBIT. Se aplican encuestas, entrevistas, revisión de documentos, análisis comparativos y observación. Para el procesamiento de los datos se utilizó el SPSS y Microsoft Excel.

Se evidenció la potencialidad del modelo COBIT por su carácter integrador.

Resultado

El procedimiento de diagnóstico está estructurado en 8 etapas.

Etapa I Conformación del equipo de trabajo.

1.1 Definir estructura del equipo de trabajo.

El equipo de trabajo está conformado por: personal especialista de gestión de TI, miembros del proceso de TI y miembros de la dirección de la empresa.

1.2 Determinar cantidad de miembros y seleccionar el personal.

Los integrantes del equipo estarán en dependencia de la organización y de las capacidades y experiencia de los miembros a seleccionar, pero es recomendable que quede conformado por miembros internos y externos de especialistas en la gestión de TI.

Asignación de responsabilidades y tareas a realizar como:

- Organizar y dirigir la realización de cada etapa del procedimiento (Jefe del equipo).
- Recopilar la información necesaria para desarrollar cada una de las etapas.
- Aplicar las herramientas diseñadas y realizar los cálculos establecidos.

1.3 Capacitación del equipo de trabajo.

Capacitar en temáticas referentes a la gestión de TI, el modelo COBIT y herramientas a utilizar.

Etapa II. Caracterización general de la empresa.

2.1 Describir los datos generales de la empresa.

2.2 Identificar los objetivos y procesos del negocio.

Etapa III. Análisis de los recursos de las TI y su alineación a los objetivos de

No	Recurso	Clasificación			Descripción	Proceso Relacionado	Impacto		
		Aplicación	Infraestructura	Personal			Fuerte	Medio	Débil

negocio de la empresa.

3.1 Efectuar un inventario de los recursos de las TI de la empresa.

Tabla 1: Modelo de inventario para los recursos de las TI [Fuente: elaboración propia]

Se identifican los recursos de las TI: aplicaciones, infraestructura y el personal; apoyados en el modelo que aparece en la tabla1.

3.2 Clasificar los recursos de TI en función de su impacto en el negocio.

A partir del inventario de los recursos de TI de la empresa se procede a efectuar la clasificación de los mismos, con apoyo del mecanismo que se ilustra en la figura 1.

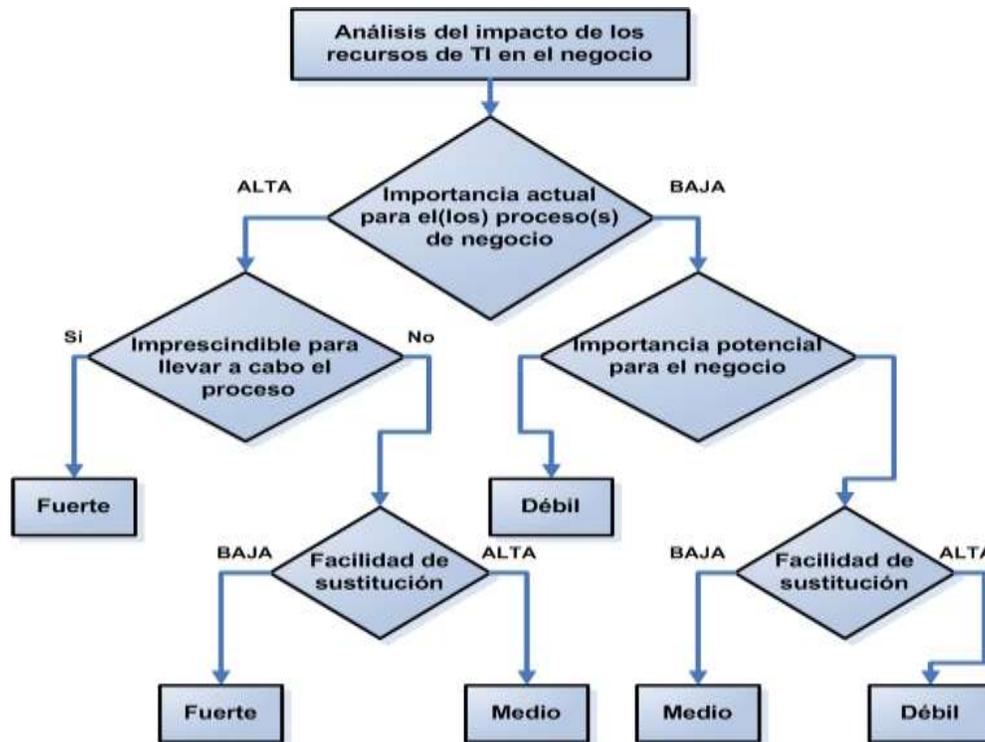


Figura 1. Mecanismo para la clasificación de los recursos de las TI en función de su impacto en el negocio [Fuente: elaboración propia]

Clasificación general por cada tipo de recurso, calculando el índice relativo, empleando la expresión1.

$$IRR_{ij} = \frac{\sum_1^m NC_{ji}}{\sum_1^n NR_i} \times 100$$

Expresión1

Donde:

IRR_{ij} ¹: Índice relativo del recurso tipo "i" según clasificación "j".

$\sum_1^m NC_{ji}$: Valor total de clasificaciones "j" del recurso tipo "i".

¹ Índice relativo correspondiente al tipo de recurso.

$\sum_1^n NR_i$: Valor total de recursos tipo "i"

i: tipo de recurso (aplicación, infraestructura, personal).

j: clasificación del impacto (fuerte, medio, débil).

Para obtener una visión global del impacto de los recursos de las TI se propone calcular el indicador de la expresión 2.

$$IRTI_j = \frac{\sum_1^m NC_j}{\sum_1^n NRTI} \times 100$$

Expresión 2

Donde:

$IRTI_j^2$: Índice relativo de los recursos de las TI según clasificación "j".

$\sum_1^m NC_{ji}$: Valor total de clasificaciones "j".

$\sum_1^n NRTI$: Valor total de recursos de las TI.

j: clasificación del impacto (fuerte, medio, débil).

De manera similar la clasificación global estará dada por el mayor índice obtenido, determinándose si el impacto de los recursos de las TI en el negocio es Fuerte, Medio o Débil.

3.3 Evaluar los procesos de negocio en función de su grado de dependencia de las TI.

Definir el grado de dependencia de las TI en tres niveles:

- **Fuerte:** La existencia de las TI determina la ejecución de los procesos de negocio, son indispensables para obtener el producto o servicio brindado.
- **Medio:** Las TI añaden valor en el proceso de negocio, y son enfocadas en productos y servicios que sirven de apoyo.
- **Débil:** Las TI son enfocadas en los componentes de tecnología.

² Índice relativo del recurso TI según clasificación.

3.4 Analizar la correspondencia entre los recursos de las TI y los requerimientos de la empresa en función de sus objetivos de negocio.

Una vez realizada la clasificación de los recursos en función de su impacto en el negocio y la evaluación de los procesos en función del grado de dependencia de las TI, se diagnostica la situación actual de la empresa apoyados en la matriz que se muestra en la tabla 2.

DEPENDENCIA DE LOS PROCESOS DE NEGOCIO	IMPACTO DE LOS RECURSOS DE LAS TI		
	FUERTE	MEDIO	DÉBIL
FUERTE	Alineación Mantener / Mejorar gestión de TI	Alineación inadecuada Valorar proyectos de inversión / Análisis costo - beneficio	No hay alineación Ejecutar proyectos de inversión / Análisis costo - beneficio
MEDIO	Alineación inadecuada Innovación con TI / Identificar oportunidades que ofrecen los recursos de TI para el negocio	Alineación Mantener/mejorar gestión de TI	No alineación Valorar proyectos de inversión / Análisis costo - beneficio
DÉBIL	No alineación Uso de TI poco estructurado y poco emprendedor / Identificar mejoras de proceso	No alineación Valorar mejoras de procesos / Aprovechar las potencialidades de TI	Alineación Mejorar procesos / Identificar oportunidades que TI puede ofrecer al negocio

Tabla 2. Matriz dependencia de procesos de negocio / impacto de recursos de TI, análisis de alineación [Fuente: Elaboración propia]

Etapa IV. Análisis de los riesgos de las TI y su administración.

Se realiza en el análisis apoyado en la figura 2.

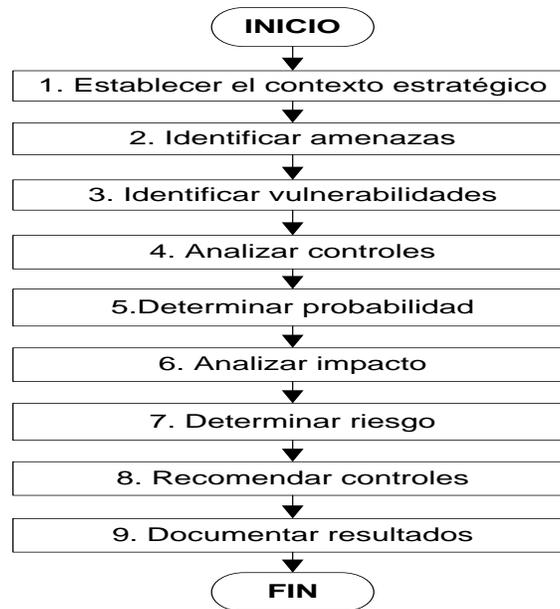


Figura 2. Procedimiento para la valoración del riesgo de TI. [Fuente: elaboración propia]

4.1 Establecer el contexto estratégico de riesgos.

A partir de la clasificación realizada en la etapa anterior, se determinaron los recursos: impacto fuerte y críticos, sobre los objetivos del negocio.

4.2 Identificar amenazas.

Amenazas naturales: inundaciones, terremotos, ciclones, desprendimientos de tierra, avalanchas, tormentas eléctricas y otras.

Amenazas medioambientales: fallas eléctricas a largo plazo, contaminación, químicos, derrame de líquidos, y otras.

Amenazas humanas: eventos que pueden ser facilitados o causados por seres humanos.

4.3 Identificar vulnerabilidades.

Debe identificarse el listado de vulnerabilidades de las TI, técnicas o no, que pueden ser explotadas por las fuentes de amenazas.

4.4 Analizar controles.

Se analizan los controles que han sido implementados en la empresa; para minimizar las probabilidades de que las amenazas actúen sobre las vulnerabilidades. El resultado de este paso es una lista de los controles existentes y el análisis de su efectividad.

4.5 Determinar nivel de probabilidad.

Para determinar la probabilidad de ocurrencia debe considerarse el resultado de las fuentes de amenazas, las vulnerabilidades, y la existencia y efectividad de controles. Las definiciones son las expresadas en la tabla 2.

4.6 Analizar impacto.

Se determina el impacto negativo sobre el negocio, de que una amenaza actúe exitosamente sobre una vulnerabilidad. Este análisis parte de la identificación de recursos críticos realizada en el primer paso.

Nivel de Probabilidad	Definición
Alto	La fuente de amenaza es altamente motivada y suficientemente capaz, y los controles para prevenir las vulnerabilidades una vez sea ejercida la amenaza son inefectivos.
Medio	La fuente de amenaza es motivada y capaz, pero los controles establecidos pueden impedir que la amenaza actúe exitosamente sobre la vulnerabilidad.
Bajo	La fuente de amenaza carece de motivación o capacidad, o los controles establecidos previenen total o al menos significativamente que la vulnerabilidad sea ejercida.

Tabla 3. Escala de nivel de probabilidad para la valoración del riesgo de TI. [Fuente: elaboración propia]

Existen impactos que no pueden ser medidos en términos cuantitativos pero pueden ser calificados o descritos en términos de impacto Alto, Medio y Bajo.

4.7 Determinar nivel de riesgos.

El objetivo de este paso es determinar el nivel de riesgo para cada par amenaza/vulnerabilidad, en función del nivel de probabilidad y la magnitud del impacto. Se puede emplear la expresión³ para determinar el nivel de riesgo, y es necesario definir

las escalas correspondientes para clasificar el resultado en Alto, Medio o Bajo; en función del riesgo analizado y la empresa donde se aplique.

$$NR = NP * MI$$

Expresión3

Donde:

NR: Nivel de Riesgo ($1 \leq NR \leq 100$)

NP: Nivel de Probabilidad ($0 \leq NP \leq 1$)

Magnitud del impacto	Definición
Alto	Que la vulnerabilidad sea ejercida (1) puede resultar en pérdidas altamente costosas de recursos importantes; (2) puede significativamente violar, dañar o impedir la misión organizacional, su reputación u otro interés; o (3) puede

MI: Magnitud de Impacto ($1 \leq MI \leq 100$)

Si la determinación del nivel de riesgo fuese solo cualitativa, a partir de las escalas definidas en los dos pasos anteriores, se propone emplear la matriz de la tabla 5. Si se considera necesario, en función del nivel de detalle deseado para la clasificación de los riesgos en la organización; la matriz propuesta puede ser extendida incorporando las clasificaciones Muy Alto y Muy Bajo en las escalas definidas en los pasos 5 y 6.

	resultar en lesiones graves o muerte de personas.
Medio	Que la vulnerabilidad sea ejercida (1) puede resultar en pérdidas costosas de recursos; (2) puede violar, dañar o impedir la misión organizacional, su reputación u otro interés; o (3) puede resultar en lesiones leves a personas.
Bajo	Que la vulnerabilidad sea ejercida (1) puede resultar en pérdidas de algunos recursos; (2) puede perceptiblemente afectar la misión organizacional, su reputación u otro interés.

Tabla 4. Escala de magnitud de impacto para la valoración del riesgo de TI. [Fuente: elaboración propia].

Nivel de probabilidad	Magnitud del impacto		
	Bajo	Medio	Alto
Alto	Bajo	Medio	Alto
Medio	Bajo	Medio	Medio
Bajo	Bajo	Bajo	Bajo

Tabla 5. Matriz para determinar nivel de riesgo de TI. [Fuente: elaboración propia].

Alto: existe una fuerte necesidad de establecer medidas correctivas inmediatamente.

- **Medio:** se necesitan acciones correctivas, debe desarrollarse un plan para implementarlas en un período razonable de tiempo.
- **Bajo:** debe determinarse si se necesitan acciones correctivas o se decide aceptar el riesgo.

4.8 Recomendar controles

En este paso deben recomendarse los controles que puedan mitigar o eliminar los riesgos identificados.

4.9 Documentar resultados

Los resultados de este procedimiento específico deben documentarse como un breve reporte que incluya las fuentes de amenaza y vulnerabilidades identificadas, los riesgos evaluados y los controles recomendados.

Etapa V. Caracterización del grado de satisfacción de los trabajadores con los recursos y servicios de las TI

5.1 Encuesta de satisfacción del personal con los recursos y servicios de las TI.

Área de trabajo: _____

Categoría ocupacional _____

Definición de respuestas: S= Satisfecho, MS= Medianamente Satisfecho, I= Insatisfecho

Definición de respuestas: A= Alta, M= Media, B= Baja

1. Con relación a la infraestructura de TI, señale en qué medida se encuentra usted satisfecho con:

S MS I

a) La calidad de la infraestructura de TI que usted utiliza.

b) Disponibilidad de la infraestructura de TI para realizar su trabajo.

c) La correspondencia entre las características de la infraestructura de TI y sus necesidades de trabajo.

2. En relación a los programas facilitados por la empresa para apoyar su trabajo, señale en qué medida se encuentra usted satisfecho con:

S MS I

a) La calidad de los softwares de las TI.

b) La correspondencia entre las funcionalidades que brindan los programas y sus necesidades de trabajo.

c) Disponibilidad de la información que ofrecen los sistemas de las TI existentes.

3. Valore de manera general la calidad de los siguientes servicios de las TI provistos por la empresa.

A M B

a) Servicios de correo.

- b) Servicios de conectividad.
- c) Internet.
- d) FTP (Protocolo de Transferencia de Ficheros).
- e) Antivirus.
- f) Actualizaciones de SO Windows.
- g) Señale otros y valore.

4. Con relación a los servicios de TI que provee la empresa para apoyar su trabajo, señale en qué medida se encuentra usted satisfecho con:

S MS I

- a) Correspondencia entre los servicios que se ofrecen y sus necesidades de trabajo.
- b) La disponibilidad de los servicios.
- c) La calidad de los mantenimientos que recibe su activo informático.
- d) La frecuencia de los mantenimientos que recibe su activo informático.

5. Señale en qué medida se encuentra usted satisfecho con los aspectos siguientes:

S MS I

- a) La atención que le brinda el personal de TI a partir del tiempo que demora en dar respuesta a sus solicitudes por interrupción.
- b) Los mecanismos para reportar los problemas e incidencias relacionados con las TI.
- c) La capacitación que se le brinda para usar las TI en su puesto de trabajo.
- d) La correspondencia entre la capacitación brindada y sus necesidades

reales.

e) El interés de la dirección de la empresa con respecto a la capacitación para el uso de las TI.



f) La existencia de manuales de ayuda u otra documentación para apoyar el uso de las aplicaciones de las TI.



6. ¿Su jefe inmediato superior acepta las sugerencias que Ud. y sus compañeros le hacen respecto al uso y necesidad de las TI para su trabajo?

Siempre

En ocasiones

Nunca

7. La empresa ha evaluado antes su opinión sobre la calidad de los recursos y servicios de las TI?

Sí

No

8. Su satisfacción con los recursos y servicios de las TI es:

Alta

Media

Baja

9. A continuación puede emitir cualquier sugerencia u opinión que Ud. desee expresar, con relación a la gestión de los recursos y servicios de las TI en su empresa.

Etapa VI. Realización del diagnóstico de madurez de los objetivos de control de las TI.

Pasos del diagnóstico de madurez:

1. Definir los dominios y objetivos de control a diagnosticar.
2. Realizar la recopilación, verificación y análisis de información.
3. Determinar el nivel de madurez de cada objetivo de control.

6.1 Definir los dominios y objetivos de control a diagnosticar.

Se definen los dominios a diagnosticar y los objetivos de control correspondientes a cada dominio apoyados en la tabla 6.

Dominios a diagnosticar	Objetivos de control correspondientes a cada dominio
Planificación y Organización	Definir el plan estratégico de TI. Definir la arquitectura de la información Determinar la dirección tecnológica. Definir procesos, organización y relaciones de TI. Administrar la inversión en TI. Comunicar las aspiraciones y la dirección de la gerencia. Administrar recursos humanos de TI. Administrar calidad. Evaluar y administrar riesgos Administrar proyectos
Adquisición e Implantación	Identificar soluciones automatizadas. Adquirir y mantener el software aplicativo. Adquirir y mantener la infraestructura tecnológica Facilitar la operación y el uso. Adquirir recursos de TI. Administrar cambios. Instalar y acreditar soluciones y cambios.
Entrega y soporte	Definir y administrar niveles de servicio. Administrar servicios de terceros. Administrar desempeño y capacidad. Garantizar la continuidad del servicio. Garantizar la seguridad de los sistemas. Identificar y asignar costos. Educar y entrenar a los usuarios. Administrar la mesa de servicio y los incidentes. Administrar la configuración. Administrar los problemas. Administrar los datos.

	Administrar el ambiente físico. Administrar las operaciones.
Monitoreo y evaluación	Monitorear y evaluar el desempeño de TI. Monitorear y evaluar el control interno Garantizar cumplimiento regulatorio. Proporcionar gobierno de TI.

Tabla 6. Dominios para el diagnóstico. [Fuente: ISACA (2007)]

6.2 Determinar el nivel de madurez de cada objetivo de control

El equipo debe asignar una calificación al comportamiento de cada objetivo de control diagnosticado, que estará dada en una escala de medición creciente de 0 (no existente) hasta 5 (optimizado). [ISACA (2007)]

<p>0 No existente. La empresa no ha reconocido siquiera que existe un problema a resolver.</p> <p>1 Inicial. Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. El enfoque general hacia la administración es desorganizado.</p> <p>2 Repetible. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.</p> <p>3 Definido. Es poco probable que se detecten desviaciones.</p> <p>4 Administrado. Se usa la automatización y herramientas de una manera limitada o fragmentada.</p> <p>5 Optimizado. Las TI se usan de forma integrada para automatizar el flujo de procesos, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.</p>

Cuadro 1. Modelo genérico de madurez. [Fuente: ISACA (2007)].

Etapa VII Evaluación de la gestión de TI en la empresa.

Evaluación de la gestión de TI en la empresa, se utiliza el indicador **Nivel de la Gestión de TI (I_{GTI})** a través de:

1. Determinación de la importancia relativa de los dominios y objetivos de control.

2. Evaluación de los dominios y objetivos de control.
3. Determinación del indicador I_{GTI} . Representación gráfica de los resultados.
4. Elaboración del informe de evaluación.

7.1 Determinación de la importancia relativa de los dominios y objetivos de control.

Se propone utilizar el método de ordenación simple. La determinación de pesos consta de tres momentos los cuáles se describen a continuación:

7.1.1 Asignación a los dominios y objetivos de control de un orden de prioridad

Los expertos asignan a los dominios y objetivos de control un orden de prioridad, “de 1 a 4” según la preferencia o nivel de importancia que poseen para el evaluador, de forma tal que el valor “1” representará el de menor importancia en la gestión de TI.

7.1.2 Análisis de la concordancia en el juicio de los expertos

Se utiliza el coeficiente de concordancia de Kendall y la prueba de hipótesis correspondiente.

Coeficiente de concordancia de Kendall.

H0: no existe asociación entre el juicio de los expertos.

H1: Existe asociación entre el juicio de los expertos.

$$W = \frac{S}{\frac{1}{12}K^2 (N^3 - N)}$$

Expresión4

Donde:

S: suma de los cuadrados de las desviaciones observadas de la media de R_j

R_j : suma de rangos asignados a cada solicitante.

k : número de conjuntos de rangos u ordenaciones.

N: número de entidades (objetos, individuos, factores) ordenados.

$$S = \sum_{j=1}^k \left(R_j - \frac{\sum R_j}{N} \right)^2$$

Expresión5

Máxima suma posible de las desviaciones al cuadrado, es decir, la suma S que ocurrirá al darse un perfecto acuerdo entre las k ordenaciones.

- Prueba de la significación de W

Para muestras pequeñas $N < 7$: RC: Si $S \geq S^*$ (tabulada), se rechaza la hipótesis de nulidad

Para muestras grandes $N > 7$

Estadígrafo: $X^2 = K(N-1)W$

RC: Si $X^2 \geq X^2$ tabulada, se rechaza la hipótesis de nulidad.[Fuente: Siegel 1972]

7.1.3 Determinación del peso de los dominios y de los objetivos de control

De comprobar la existencia de concordancia entre los expertos, se ordenan definitivamente los dominios y objetivos de control dado por el valor de las sumas de rango. Con este orden definitivo se calcula el peso de los dominios (W_g) y objetivos de control (W_{dg}), a través del método de ordenación simple que es el método de cálculo de peso que se recomienda utilizar.

7.2 Evaluación de los dominios y objetivos de control

Se propone la evaluación de cada objetivo de control a través de la expresión siguiente:

$$EOC_{dg} = \frac{W_{dg} \cdot x_{NM_{dg}}}{5}$$

Expresión6

Donde:

EOC_{dg} ³: Evaluación del objetivo de control correspondiente al dominio g.

W_{dg} : Peso del objetivo de control correspondiente al dominio g.

³ Evaluación del objetivo de control de la empresa.

NM_{dg} : Nivel de madurez del objetivo de control d correspondiente al dominio g.

La suma de las evaluaciones de los objetivos de control dará el resultado del dominio, esto es:

$$RD_g = \sum_{d=1}^{m_g} EOC_{dg}$$

Expresión7

Donde:

RD_g : Resultado del dominio g.

$d = \overline{1, m_g}$ Siendo m la cantidad de objetivos de control por cada dominio g.

La evaluación de cada uno de los dominios se calculará según la expresión siguiente:

$$ED_g = W_g \times RD_g \times 100$$

Expresión8

Donde:

ED_g : Evaluación del dominio g.

W_g : Peso del dominio g.

7.3 Determinación del indicador I_{GTI} y representación gráfica de los resultados.

Para la evaluación de la gestión de TI se propone el indicador Nivel de la Gestión de TI (I_{GTI})⁴ en la expresión7:

$$I_{GTI} = \sum_{g=1}^4 ED_g$$

Expresión7

Intervalos de I_{GTI} (%)	Evaluación de la gestión de TI
$(95 \leq I_{GTI} \leq 100)$	Nivel 5: OPTIMIZADO

⁴ Indicador Nivel de gestión de la Tecnologías de la información de la empresa.

$(75 \leq I_{GTI} < 95)$	Nivel 4: ADMINISTRADO
$(55 \leq I_{GTI} < 75)$	Nivel 3: REPETIBLE
$(35 \leq I_{GTI} < 55)$	Nivel 2: DEFINIDO
$(15 \leq I_{GTI} < 35)$	Nivel 1: INICIAL
$(I_{GTI} < 15)$	Nivel 0: NO EXISTENTE

Tabla7. Escala para la evaluación de la gestión de las TI.[fuente: elaboración propia].

7.4 Elaboración del informe de evaluación.

A partir de los resultados obtenidos en las etapas precedentes se elabora un informe donde se relacionen los dominios y objetivos de control que reflejaron mayores dificultades, se identifican los principales problemas que afectan la gestión de las TI en la empresa.

Etapa VIII Propuesta de medidas correctivas, preventivas y/o de mejora.

Una vez obtenida la evaluación de la gestión de TI, el informe elaborado por el equipo de trabajo puede indicar la necesidad de acciones correctivas, preventivas y/o de mejora, según sea aplicable, en el cual se elabora la propuesta de las acciones.

Ejemplo: Aplicación del procedimiento para el diagnóstico de la gestión de las Tecnologías de la Información (TI), en una empresa comercializadora de combustibles.

Etapa III. Análisis de los recursos de las TI y su alineación a los objetivos de negocio de la empresa.

3.1 Efectuar un inventario de los recursos de las TI de la empresa.

Se clasifica de impacto global según Expresión1 y Expresión2. Se aprecia que el impacto global fue calificado de Débil. El recurso que tiene mayor cantidad de impactos fuertes es la infraestructura donde de un total de 77 tienen un impacto Fuerte 22, lo que representa el 28.6 %. Las aplicaciones son clasificadas de Medio en el 36.36% de los casos. Y en caso de los recursos de personal se clasifica Fuerte.

3.2 Clasificar los recursos de TI en función de su impacto en el negocio.

Índice relativo	Resultados de los índices según clasificación j	Clasificación
Global (IRT _i)	Fuerte = 30.65	DÉBIL
	Medio = 29.19	
	Débil = 40.14	
IRR _{ij} Personal	Fuerte = 60	Fuerte
	Medio = 20	
	Débil = 20	
IRR _{ij} Aplicaciones	Fuerte = 30.9	Medio
	Medio = 36.36	
	Débil = 32.74	
IRR _{ij} Infraestructura	Fuerte = 28.6	Débil
	Medio = 24.6	
	Débil = 46.8	

Figura 2. Clasificación los recursos de TI en función de su impacto en el negocio.

Etapa VII Evaluación de la gestión de TI en la empresa.

Se realizan los cálculos de forma manual e incluyen los cálculos de pesos, la evaluación de los dominios W_g^5 y objetivos de control W_{dg}^6 y el cálculo del indicador global con su correspondiente evaluación.

7.1 Determinación de la importancia relativa de los dominios y objetivos de control.

Se determina la importancia relativa de los dominios y objetivos de control apoyados en la siguiente tabla.

CONCLUSIONES

Se constatan escasos procedimientos e indicadores que permitan diagnosticar el estado de la gestión de TI en una organización, considerándose la investigación actual y pertinente.

El estudio realizado confirma la existencia creciente de estándares y marcos de trabajo sobre la gestión de las TI, sus diversas prácticas y la importancia de su evaluación, así como el papel protagónico de los procedimientos e indicadores que permiten diagnosticar el estado de la gestión de TI en una empresa.

Se evidencia la inclusión de las TI en la estrategia de negocio empresarial para potenciar las oportunidades de negocio y los indicadores que permitan evaluar el desempeño y la capacidad de los recursos de TI.

Se realiza la propuesta de un procedimiento de diagnóstico de la gestión de las TI en las empresas, para determinar oportunidades de mejora que contribuyan a evaluar los

⁵ Cálculo de peso de los dominios.

⁶ Cálculo de peso de los objetivos de control.

riesgos y beneficios asociados con TI y el impacto de las mismas en el logro de los objetivos empresariales.

BIBLIOGRAFÍA

ISACA. (2007). COBIT 4.1 IT Governance Institute. Extraído de:

<http://www.isaca.org>. Consulta: 11/05/16

ISO/IEC 27001 (2005). Information technology - Security techniques - Information security management systems – Requirements. Extraído de:

<http://www.iso.org/iso/catalogue>. Consulta: 6/07/16

ISO/IEC 27002 (2005). Information technology - Security techniques - Code of practice for information security management. Extraído de:

<http://www.iso.org/iso/catalogue>. Consulta: 6/07/16

ISO/IEC 27005 (2008). Information technology -- Security techniques -- Information security risk management. Extraído de:

<http://www.iso.org/iso/catalogue>. Consulta: 6/07/16

ISO/IEC 38500 (2008). Corporate Governance of Information Technology. Extraído de:

<http://www.iso.org/iso/catalogue>. Consulta: 6/07/16

Jones, Jack A. (2015). An Introduction to Factor Analysis of Information Risk (FAIR). A framework for understanding, analyzing, and measuring information risk. Risk Management Insight.

ITGI (2009). ITGI Enables ISO/IEC 38500:2008 Adoption. IT Governance Institute IT Risk Management Report Volumen 1 (2007). Symantec. Trends through December 2009. Disponible en <http://www.symantec.com>

Van Grembergen, Win & De Haes, Steven (2009) Enterprise Governance of Information Technology. Achieving Strategic Alignment and Value. Springer e-ISBN 978-0-387-84882-2.

López Paz, Carlos R (2015). “Un acercamiento a la alineación de las tecnologías de la información con el negocio”. Ponencia en el evento virtual del taller internacional las TIC en la gestión de las organizaciones. Informática 2015. Disponible en: <http://www.informaticahabana.cu/>

