UNIVERSIDAD CENTRAL "MARTA ABREU" DE LAS VILLAS
VERITATE SOLA NOBIS IMPONETUR VIRILISTOGA. 1948
FACULTAD DE INDUSTRIAL Y TURISMO
Departamento de Ingeniería Industrial

Trabajo de Diploma

Título: Aplicación del procedimiento de diagnóstico de la gestión de las Tecnologías de la Información en las empresas TECNOAZUCAR y ATI V.C

Autora: Diana Pérez Hernández

Tutores: Ms.C. Patricia Pérez Lorences
Ms.C. Frank Medel González

Curso 2011-2012

Resumen

Para lograr que las tecnologías de la información (TI) contribuyan de manera efectiva al cumplimiento de los objetivos de negocio de una empresa, se hace necesario evaluar la gestión de estos recursos. En la presente investigación se aplica en las empresas UEB Villa Clara TECNOAZUCAR y Tecnología de la Información y Automatización (ATI) de Villa Clara, el procedimiento propuesto por Pérez Lorences (2010) para diagnosticar el estado actual de la gestión de TI en una organización. Se calcula el indicador nivel de la gestión de tecnologías de la información (I_{GTI}) en ambas empresas que se basa en el modelo COBIT y la evaluación de madurez de procesos de TI en una organización. La aplicación del procedimiento y los instrumentos metodológicos asociados permitió la determinación de los problemas que afectan la gestión de TI en estas empresas, así como la determinación de oportunidades de mejora que favorezcan la comprensión y evaluación de los riesgos y beneficios asociados con TI y el impacto de las mismas en el logro de sus objetivos empresariales.

Summary

To ensure that information technology (IT) effectively contributes to meeting the business objectives of a company, it is necessary to evaluate the management of these resources. In this research applies the procedure proposed by Pérez Lorences (2010) to diagnose the current state of IT management in an organization, in UEB Villa Clara TECNOAZUCAR and Information Technology and Automation (ATI) of Villa Clara. It calculates the level of the management of information technology (IGTI) in both companies based on the COBIT model and evaluation of IT process maturity in an organization. The application of the procedure and the associated methodological tools allowed the identification of problems affecting the management of IT in these companies, as well as identifying opportunities for improvement to promote the understanding and assessment of the risks and benefits associated with IT and the impact of them in achieving their business goals.

Índice

Introducción.....1

Capítulo 1. Construcción del marco teórico referencial.....5

1.1. Definición de TI..... 5

1.2. Definición de gestión de TI (GTI)..... 7

1.3. Metodologías, estándares y marcos de trabajo para la GTI..... 10

1.3.1. Estándares ISO de Seguridad de la Información..... 10

1.3.2. Estándares ISO de Gestión de TI..... 11

1.3.3. Biblioteca de Infraestructura de Tecnologías de la Información (ITIL, Information Technology Infrastructure Library)..... 13

1.3.4. Cuadro de mando integral de las TI. (IT BSC)..... 14

1.3.5. Objetivos de Control para Tecnología de Información (COBIT, Control Objectives for Information and related Technology)..... 14

1.4. Alineación de la TI al negocio..... 16

1.5. Gestión de riesgos..... 19

1.6. Evaluación de la GTI..... 21

1.7. Experiencias en el mundo y Cuba..... 22

1.8. Conclusiones parciales..... 25

Capítulo 2. Procedimiento para diagnosticar la gestión de TI.....26

2.1. Procedimiento para diagnosticar el estado actual de la gestión de TI..... 26

2.2. Caracterización de las empresas objeto de estudio..... 41

2.2.1. UEB de Ingeniería y Servicios Técnicos Azucareros (TECNOAZUCAR VC) 41

2.2.2. Empresa de Tecnología de la Información y Automática (ATI)..... 42

2.3. Conclusiones parciales..... 45

Capítulo 3. Aplicación del procedimiento en las empresas.....46

3.1. Aplicación del procedimiento en las empresas objeto de estudio..... 46

3.1.1. Desarrollo de las etapas 1 y 2..... 46

3.1.2. Etapa 3: Análisis de los recursos de TI y su alineación a los objetivos de negocio de la organización..... 47

3.1.3. Etapa 4: Análisis de los riesgos de TI y su administración 48
3.1.4. Etapa 5: Caracterización del grado de satisfacción de los trabajadores con los recursos y servicios de TI 49
3.1.5. Etapa 6: Realización del diagnóstico de madurez de los objetivos de control ... 50
3.1.6. Etapa 7: Evaluación de la gestión de TI en la organización 60
3.1.7. Etapa 8: Propuesta de medidas correctivas, preventivas y/o de mejora 64
3.2. Conclusiones parciales 66
Conclusiones generales 67
Recomendaciones 68
Bibliografía 69

Introducción

Las tecnologías de la información (TI) son un elemento imprescindible y en continuo desarrollo dentro de cualquier empresa. Agregan valor a las actividades operacionales y de gestión empresarial, permitiendo a las empresas obtener ventajas competitivas, permanecer en el mercado y centrarse en su negocio. Utilizando eficientemente las TI se pueden obtener ventajas competitivas, pero es preciso encontrar procedimientos acertados para mantener tales ventajas, así como disponer de cursos y recursos alternativos de acción para adaptarlas a las necesidades del momento, pues las ventajas no siempre son permanentes.

Las TI son esenciales para mejorar la productividad de las empresas, la calidad, el control y facilitar la comunicación y la toma de decisiones, entre otros beneficios; pero su aplicación debe llevarse a cabo de forma inteligente y por ende es vital una adecuada gestión ya que su uso está cambiando la forma tradicional de hacer las cosas. En ocasiones la existencia de las TI determina totalmente la ejecución de los procesos de negocio de una empresa, en otras, pueden convertirse en un elemento diferenciador para los resultados obtenidos por el negocio, aumentando la calidad y efectividad del bien o servicio brindado; o por otro lado, pueden verse como un elemento para facilitar la realización de algunas actividades de apoyo.

En un mundo tan cambiante, la alta dirección se está dando cuenta del impacto significativo que la información puede tener en el éxito de una empresa. La dirección espera un alto entendimiento de la manera en que la tecnología de información es operada y de la posibilidad de que sea aprovechada con éxito para tener una ventaja competitiva. Es por ello que la gestión efectiva de las TI de una empresa ayuda a garantizar que TI soporte las metas del negocio, optimice la inversión del negocio en TI, y se administren de forma adecuada los riesgos y oportunidades asociados a estos recursos.

Para las empresas es importante conocer el estado actual de la gestión de estos recursos en función de identificar los problemas que tienen y cómo solucionarlos. De ahí que es imprescindible llevar a cabo estudios que satisfagan esta necesidad.

En la empresa UEB Villa Clara TECNOAZUCAR, encargada de producir y comercializar productos y servicios de excelencia, generados por el desarrollo y la diversificación de la

agroindustria azucarera, las TI desempeñan un rol importante y se han evidenciado problemas con relación a la gestión de estos recursos. Entre estos, es posible señalar:

- la inadecuada capacitación del personal para el manejo de estos recursos

- la falta de documentación de ayuda que facilite el uso de los sistemas

- inadecuado control de acceso a los locales

- existen fallas de fluido eléctrico frecuentemente y no existen mecanismos para realizar salvas de las informaciones. Esto puede provocar la pérdida de datos de los sistemas de información y dejar la empresa sin información vital para su funcionamiento, lo que puede derivar en pérdidas financieras, de tiempo y de desarrollo empresa, así como de su seguridad física y gestión

- se evidencia falta de control de la aplicación del plan de Seguridad Informática y hechos que demuestran su violación.

La empresa de Tecnología de la Información y Automatización (ATI) de Villa Clara está encargada de prestar servicios integrales de ingeniería y proyectos en la rama de la instrumentación y la automatización industrial. En esta empresa los recursos de TI son imprescindibles y se ha establecido la necesidad de mejorar su gestión para lograr un mayor alineamiento a sus objetivos de negocio y administrar adecuadamente sus riesgos.

Todo lo anterior evidencia la necesidad de llevar a cabo estudios diagnósticos de la gestión de TI que permitan evaluar el nivel de gestión de TI en estas empresas y trazar estrategias adecuadas de mejoramiento, por lo que la **situación problemática** de esta investigación estará dada por los problemas antes señalados que evidencian la contradicción existente entre la necesidad que tiene la dirección de las empresas UEB Villa Clara TECNOAZUCAR y Tecnología de la Información y Automatización (UEB ATI), de comprender y evaluar los riesgos y beneficios asociados con las TI y la falta de estudios para diagnosticar el estado actual de su gestión.

El **problema científico** queda conformado como sigue a continuación: los directivos de la empresa UEB Villa Clara TECNOAZUCAR y la empresa de Tecnología de la Información y Automatización (UEB ATI) carecen de la aplicación de herramientas, que permitan caracterizar la situación actual de ambas en la gestión de sus TI, teniendo en cuenta la

alineación de las mismas al negocio y la administración de los riesgos y beneficios asociados.

En correspondencia con lo planteado anteriormente se formuló la siguiente **hipótesis de la investigación**: a través de la implementación del procedimiento de diagnóstico de la gestión de TI, se pueden determinar los principales problemas que afectan dicha gestión en las empresas UEB Villa Clara TECNOAZUCAR y la Empresa de Tecnología de la Información y Automatización (UEB ATI); en función de erradicarlos y mejorar la comprensión y administración de los riesgos y beneficios asociados con estos recursos.

Esta hipótesis quedará comprobada si la aplicación del procedimiento general y los instrumentos metodológicos, en los objetos de estudio seleccionados; permite:

- Analizar los recursos de TI y su alineación a los objetivos de negocio identificando los problemas relacionados.
- Analizar los riesgos asociados a las TI y los problemas relativos a su administración.
- Evaluar la gestión de TI a partir del diagnóstico de sus objetivos de control.
- Proponer medidas que contribuyan a erradicar los principales problemas que se identifiquen.

Conforme con la hipótesis investigativa planteada, el **objetivo general** de la investigación consistió en diagnosticar el estado actual de la gestión de TI en las empresas "UEB Villa Clara TECNOAZUCAR" y "Empresa de Tecnología de la Información y Automatización (UEB ATI)". El objetivo general fue desglosado en los siguientes **objetivos específicos**:

1. Establecer las bases teóricas que permitan dar solución al problema científico planteado, a partir de la literatura nacional e internacional más actualizada.
2. Aplicar el procedimiento de diagnóstico para la gestión de TI en la empresa comercializadora UEB Villa Clara TECNOAZUCAR y la Empresa de Tecnología de la Información y Automatización (ATI).
3. Proponer las medidas correctivas, preventivas y/o de mejora que contribuyan a erradicar o mejorar los problemas detectados a partir de la implementación del procedimiento.

En el desarrollo de esta investigación se utilizaron métodos y técnicas empíricas como: encuestas, entrevistas, análisis de documentos, análisis comparativos, observación y criterio de expertos. Además se emplearon métodos teóricos como el analítico sintético, inductivo deductivo, la modelación y el enfoque sistémico estructural. Al mismo tiempo se aplicaron métodos estadísticos y matemáticos entre los cuales se encuentran el ANP como método para la asignación de pesos, y el alfa de Cronbach y análisis de frecuencias para el procesamiento de encuestas. Para el tratamiento computacional de los datos se utilizó el SPSS, el Microsoft Excel y el Super Decissions.

Para su presentación, esta tesis se estructuró en tres capítulos. El Capítulo1 define, en lo fundamental, el marco teórico - referencial de la investigación sobre las temáticas: tecnologías de la información (TI), gestión de TI, metodologías y buenas prácticas para la gestión de TI y su evaluación. En el Capítulo 2 se describe el procedimiento para diagnosticar el estado actual de la gestión de las TI en una organización y la caracterización de ambas empresas objetos de estudio. El Capítulo 3 contiene la aplicación del procedimiento en las empresas. Además se presenta un cuerpo de conclusiones y recomendaciones derivadas de la investigación realizada, la bibliografía consultada y finalmente un grupo de anexos de necesaria inclusión, como complemento de los resultados expuestos.

Capítulo 1. Construcción del marco teórico referencial

El presente capítulo muestra un análisis crítico de la literatura especializada y otras fuentes, con vistas a precisar los principales aspectos conceptuales involucrados en la investigación. En este sentido se consultó bibliografía especializada y actualizada tanto nacional como internacional sobre los temas a abordar acorde a lo planificado en el hilo conductor que se muestra en la figura 1.1.

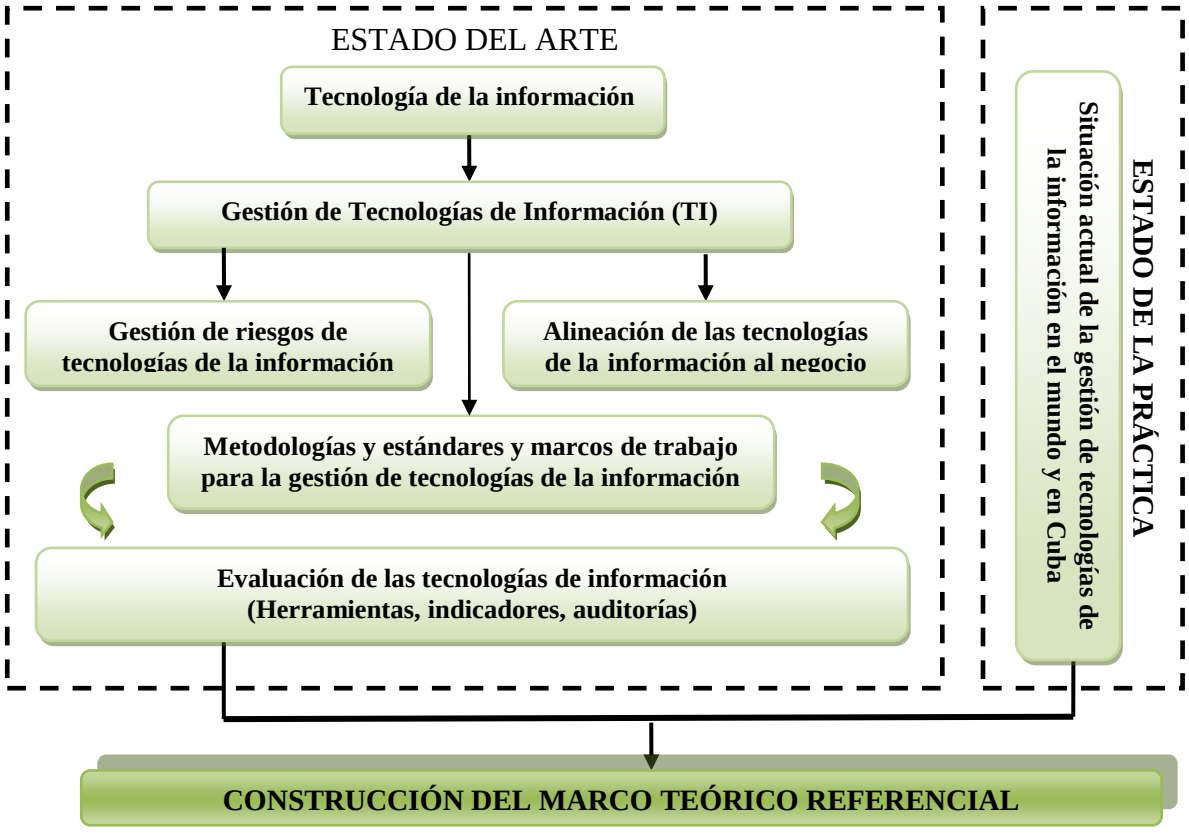


Figura 1.1. Estrategia para la construcción del marco teórico – referencial de la investigación.

1.1. Definición de TI

Las TI han sido conceptualizadas 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 [Salazar, 2011].

Según lo definido por la Asociación de la Tecnología de Información de América (ITAA, 2008) es "el estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras."

Con este enfoque tecnológico, un poco más abarcador, otro autor plantea: "Las Tecnologías de la Información se encargan del diseño, desarrollo, fomento, mantenimiento y administración de la información por medio de sistemas informáticos, para información, comunicación o ambos. Esto incluye todos los sistemas informáticos no solamente las computadoras, éstas son sólo un medio más, el más versátil, pero no el único; también las redes de telecomunicaciones, telemática, los teléfonos celulares, la televisión, la radio, los periódicos digitales, faxes, dispositivos portátiles, etc [Blogger. 2008; citado por Arias, 2009].

El concepto dado en el modelo COBIT 4.1 (2007) sin dejar de reconocer el componente tecnológico, incluye los métodos y el factor humano como recursos de TI, el mismo plantea: "Las TI han sido conceptualizadas 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" [COBIT4.1, 2007].

COBIT define cuatro tipos de recursos TI que pueden ser aplicados dentro de los procesos de TI:

- La información: se refiere a los datos en todas sus formas manejadas por los sistemas de información en cualquier forma que sea utilizada por la empresa.
- Las aplicaciones: son los sistemas de usuario automatizados y los procedimientos manuales que procesan la información.
- La infraestructura: incluye la tecnología y las instalaciones (equipo físico, funcionamiento de sistemas, las sistemas de administración de base de datos, la conexión en red, la multimedia, etcétera., y el ambiente que los aloja y respalda) y permite el procesamiento de las aplicaciones.

- Las personas: se hace referencia al personal exigido para planificar, organizar, adquirir, repartir, sostener, monitorear y valorar los sistemas de información y los servicios requeridos.

De manera similar según Berea (2006) los elementos que componen las TI son: hardware, software, procedimientos, documentos y recursos humanos.

Servicio de TI es otro concepto muy relacionado que es importante definir. Varios autores [ITIL, 2006; Reyes Retana, 2006; Berea, 2006] coinciden en que los servicios de TI son un conjunto de funcionalidades, basadas en recursos de TI, que la organización ofrece a sus clientes para llevar a cabo una función de negocio.

Las TI tienen el potencial no solamente para respaldar las estrategias existentes de la empresa, sino también concebir las nuevas estrategias. En este modo de pensar, las TI no son solamente un factor de éxito para la supervivencia y prosperidad, sino además una oportunidad de diferenciar y conseguir la ventaja competitiva [Van Grembergen & Haes, 2009].

1.2. Definición de Gestión de TI (GTI)

Numerosas definiciones del concepto *gestión de TI* han surgido a través de los años, y también se define el término *gobierno de TI*. En este epígrafe se realiza un análisis de las principales tendencias en este sentido para sentar las bases de la presente investigación.

Desde la década de los 90 el término ha recibido mucha atención y son muchos los autores que han dado desde su punto de vista diferentes definiciones acerca del mismo tales como Van Grembergen et al., (2004) que focaliza su definición en cuatro elementos básicos del gobierno de TI: alineamiento estratégico entre TI y negocio, obtención de valor de negocio a través de TI, gestión del riesgo y gestión del rendimiento. Estos elementos pueden complementarse con un quinto componente según [Webb, Pollard, Ridley], el control de cuentas. Finalmente definen gobierno de TI como la alineación estratégica de TI con el negocio de tal manera que se obtenga el máximo valor de éste a través del desarrollo y mantenimiento de efectivos controles de TI orientados al control de cuentas, a la gestión del rendimiento y con gestión del riesgo. El IT Governance Institute, (2007) introduce además en esta definición los procesos de negocio, las estructuras organizativas y el liderazgo [Fernández et al., 2011].

Coincidiendo con lo anterior [ITGI, 2008; ISACA, 2007; itSMF, 2008; citados por Luna, A. J. H de O. et al., 2010] agregan que el mismo se concentra en las TI y sus sistemas de rendimiento y en la prevención de riesgos.

La gestión de TI es utilizar y adaptar las tecnologías de forma que aporten un valor real medible, o sea, incorporar TI a la estrategia y la táctica del negocio, no solo a la operativa. Gestionar TI, es igualmente tomar las decisiones estratégicas y tácticas para aportar valor que genere beneficio [Marcos Pascual, 2005].

Este autor plantea que la GTI está en función de lograr el aporte de valor de las TI a los objetivos de negocio de la organización; pero no considera además el manejo del riesgo de TI, que debe ser también considerado como parte de la gestión. Dicho enfoque se explicita en el concepto planteado por COBIT, donde se hace referencia al término de "gobierno de TI". COBIT (2007) plantea que la necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave de la gestión de la empresa.

La necesidad de los departamentos de TI de crear valor para el negocio, ha derivado en la adopción de una gran cantidad de arquitecturas, métodos y herramientas en lo que se ha venido a denominar genéricamente como gobierno de TI. Mediante su progresiva adopción, las organizaciones están en mayor o menor medida, reduciendo los costos, procurando la ansiada alineación entre negocio por un lado y sistemas y TI por el otro [Fernández et al., 2008].

Según LeClair (2005) las principales funciones que componen la GTI son: gestionar riesgos, mejorar el servicio, gestionar costos y alinear las inversiones de TI con el negocio. Este autor plantea que para que exista una buena GTI estas funciones deben trabajar unidas para lo cual se debe llevar a cabo optimización de los servicios de negocio, gestión de los sistemas empresariales, gestión de la seguridad, gestión del almacenamiento.

Caporarello (2008) plantea que: "los objetivos del gobierno de TI son: definir las estructuras, procesos, y mecanismos para definir los derechos de la toma de decisiones y las responsabilidades sobre los principales problemas de TI; controlar y monitorear la

efectividad de tales decisiones, y mitigar los riesgos relacionados con TI en función de lograr los objetivos de la organización."

Gobierno de TI y gobierno corporativo no pueden ser considerados como disciplinas puras distintas, el gobierno de TI tiene que estar integrado en la estructura de gobierno de la empresa en conjunto. [Guldentops, 2003; ITGI, 2001; Peterson, 2003; Duffy, 2002; citados por Van Grembergen, 2004]. Por todo lo anterior es importante concluir en que gobierno de TI, es una parte esencial del gobierno corporativo y de las direcciones de la definición y la puesta en práctica de procesos, estructuras y mecanismos relacionales en la organización, que permiten tanto a la empresa como a las personas de TI ejecutar sus responsabilidades a favor de la alianza de la empresa / TI y la creación del valor de la empresa a través de las inversiones permitidas por TI [Van Grembergen & Haes, 2009].

Una relación de conceptos acerca del término de Gobierno de TI se muestra en el Anexo 1.

En la literatura consultada se establece una comparación entre gestión y gobierno de TI donde se plantea que este último es la capacidad organizativa ejercitada por la dirección de la empresa y los ejecutivos y que la gestión de TI es controlar la formulación y puesta en práctica de la estrategia de TI, y de este modo asegurar su fusión con la de la empresa. Aunque estas definiciones difieren en algunos aspectos, el enfoque es sobre los mismos asuntos: alcanzar el enlace entre la empresa y las TI, y la responsabilidad principal de la junta de directores, se demuestra también que la gestión de TI debe estar involucrada en los procesos de gobierno de TI. Sin embargo, hay una diferencia clara entre gobierno y gestión de TI. La gestión se concentra en el suministro eficaz de los servicios, los productos y la dirección de las operaciones de TI. El gobierno es mucho más amplio y se concentra en funcionar y transformar las TI para cubrir las demandas futuras actuales de la empresa y sus clientes [Van Grembergen et al., 2009; Peterson, 2003].

Estos autores dan al concepto de gestión de TI un significado más operativo y al de gobierno un enfoque estratégico. Con este significado operativo se relaciona el término gestión de servicios de TI, también muy referido en la literatura, que según itSMF (2005) e ITIL (2007) se encarga de que la provisión y soporte de servicios TI resulten apropiados a los requerimientos de negocio de la organización.

El término gestión se maneja en muchas fuentes con similar significado al de gobierno y en otras se plantea como parte de este último, o más específicamente referido a la gestión de los servicios de TI. En muchas ocasiones estas discrepancias son ocasionadas más por un problema idiomático y de traducción que conceptual; pero al encontrarse diferentes vertientes en la literatura es necesario aclarar que a efectos de esta investigación, aunque se reconoce y trabaja con las interpretaciones de ambos términos, se tratarán como sinónimos.

1.3. Metodologías, estándares y marcos de trabajo para la GTI

En la actualidad la variedad de metodologías presentes en el mercado es muy amplia y va en ascenso con la aparición cada vez más numerosa de nuevas metodologías, sin embargo en este epígrafe se muestran los principales y más referenciados en la bibliografía consultada.

1.3.1. Estándares ISO de seguridad de la información

ISO/IEC 27001:2005 *(Tecnología de información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos)*

"Especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información en el contexto de los riesgos de negocio generales de la organización. Especifica los requerimientos para la aplicación de controles de seguridad." [ISO/IEC 27001, 2005]. Según Alan Calder (2006) siguiendo el conocido "Ciclo de Deming".

Tiene como propósito reducir la vulnerabilidad de una organización a riesgos de seguridad de la información, mediante el uso de un Sistema de Gestión de la Seguridad de la Información. Se puede aplicar a las organizaciones que deseen mantener los riesgos bajo control y proteger sus activos.

ISO/IEC 27002:2005 *(Tecnología de información – Técnicas de seguridad – Código de prácticas para la gestión de seguridad de la información)*

Establece las directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización. Los objetivos señalados proveen una guía general sobre las metas comúnmente aceptadas de la gestión de seguridad de la información [ISO/IEC 27002, 2005].

El objetivo de 27002:2005 de la ISO / IEC es proveer la información a los responsables de implementar la seguridad de la información dentro de una organización. Puede ser una buena práctica para desarrollar y mantener los patrones de seguridad y las prácticas de dirección, y mejorar la confiabilidad sobre la seguridad de información en las relaciones interorganizacionales. Define 133 estrategias de controles de seguridad, bajo 11 encabezamientos muy importantes [ITGI & OGC, 2008].

ISO/IEC 27005:2008 *(Tecnología de información – Técnicas de seguridad – Gestión de los riesgos de seguridad de la información)*

Proporciona directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñado para ayudar a la aplicación satisfactoria de seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y terminologías descritas en la norma ISO/IEC 27001 y ISO/IEC 27002 es importante para una comprensión completa de la norma ISO/IEC 27005:2008. Es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tengan la intención de gestionar los riesgos que podrían comprometer la seguridad de la información de la organización [ISO/IEC 27005, 2008].

1.3.2. Estándares ISO de Gestión de TI

ISO/IEC 38500: 2008. *Corporate governance of information technology (Gobierno Corporativo de TI)*

La Organización Internacional de Normalización (ISO) publicó en el 2008 una nueva norma internacional que se define como "Gobierno Corporativo de TI". En esta norma, la ISO formula seis principios para el gobierno de las TI. Los principios expresan el comportamiento preferido para orientar la toma de decisiones relacionadas con TI y dirigir los roles y responsabilidades del negocio y de TI. Los principios son los siguientes: *la estrategia, la responsabilidad, la adquisición, el rendimiento, la conformidad y el comportamiento humano.*

Beneficio del patrón ISO / IEC 38500:

- Eleva la importancia del gobierno de TI debido a los riesgos involucrados y las inversiones importantes requeridas.
- Anima a las empresas a usar patrones apropiados para apuntalar su gobierno de TI.
- Suministra una base de seis principios básicos de ayuda a los directores para cuando evalúen, dirijan y monitoreen el uso de TI en sus empresas. Seguir estos principios los ayudará a balancear los riesgos y oportunidades alentadoras que surgen del uso de TI.
- Es aplicable para todas las empresas, desde la más pequeña hasta la más grande, a pesar de todo de la determinación, el diseño y la estructura de propiedad.
- Hace más claro que el gobierno de TI de una empresa pueda ayudar a los directores a garantizar la conformidad con las obligaciones, con respecto al uso aceptable de TI y asegurando que ese uso de TI colabora en el rendimiento de la empresa absolutamente.
- También hace más claro que un sistema de TI inadecuado pueda exponer a los directores al riesgo de no obedecer en un rango cada vez más amplio de la legislación [ITGI, 2009].

Uno de los mensajes clave de este estándar es que, debido a los gastos, riesgos y valor potencial de TI en los negocios, el consejo directivo de la empresa es responsable de asegurar que TI esté correctamente dirigido [IBM, 2008].

ISO/IEC 20000: 2005. *Information technology - Service management. (Tecnología de información –Gestión de servicios)*

Según Pérez Sánchez 2008 este es el primer estándar específico para la gestión de servicios de TI, y su objetivo es aportar los requisitos necesarios, dentro del marco de un sistema completo e integrado, que permita que una organización provea servicios TI gestionados, de calidad y que satisfagan los requisitos de negocio de sus clientes.

Tiene como propósito fomentar la adopción de un planteamiento de procesos integrados que garanticen la entrega de servicios bien gestionados que cumplan los requisitos del negocio y los clientes. Se aplica a todas las organizaciones que sus proveedores de servicios

de TI que deseen adoptar la norma global quieran demostrar que tienen la capacidad para entregar servicios de TI de calidad a clientes externos o internos.

ISO/IEC 20000-1:2005 define los requisitos para un proveedor de servicios para ofrecer servicios gestionados. Se basa en la BS 15000-2, que ha sido sustituida. Se puede utilizar (…) para proporcionar un enfoque coherente por todos los proveedores de servicios en una cadena de suministro, (…) para demostrar la capacidad para satisfacer las necesidades del cliente y para mejorar los servicios [ISO/IEC 20000-1, 2005].

ISO/IEC 20000-2:2005 representa un consenso de la industria sobre la orientación a los auditores y ofrece asistencia a los proveedores de servicios de planificación de mejoras en el servicio o para ser auditadas según la norma ISO / IEC 20000-1 [ISO/IEC 20000-2, 2005].

1.3.3. Biblioteca de Infraestructura de Tecnologías de la Información (ITIL, Information Technology Infrastructure Library)

Surge a finales de 1980, y se ha convertido en el estándar mundial de facto en la Gestión de Servicios Informáticos. (…). Hoy, ITIL es conocido y utilizado mundialmente [Colectivo, 2005].

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente [ITIL, 2006].

Se origina como una colección de libros que cubren prácticas específicas de la Gestión de Servicios de TI. La versión 3 es la más actual y fue lanzada en mayo del 2007. Está compuesta por 5 volúmenes: estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continúa del servicio. ITIL provee uno compresiva, consecuente y coherente base de buenas prácticas para el servicio de TI para que la dirección y los procesos relacionados, promocionen un enfoque de buena calidad y así conseguir la eficacia de la empresa y la eficiencia en la dirección del servicio de TI. [ITGI and OGC, 2008].

1.3.4. Cuadro de mando integral de las TI. (IT BSC)

En el grupo de los framework estratégicos se encuentra el *IT balanced scorecard* (IT-BSC por sus siglas en inglés) centrado en traducir la estrategia TI en objetivos e indicadores conectados en relaciones causa/efecto y en términos operacionales.

El modelo estándar del BSC, debía ser modificado cuando se fuese a aplicar a las TI. (…)La aplicación de BSC a las TI fue descrita por Van Grembergen & Van Bruggen (1997) y Van Grembergen & Timmerman (1998). [Van Grembergen, 2007]. Las adaptaciones realizadas por estos autores, generaron un BSC genérico para las TI.

El IT BSC tiene dos elementos singulares en relación con el BSC a un nivel organizacional [Kaplan and Norton 2006; citado por López Paz]: (1) redefinir el concepto de las cuatro perspectivas ―financiera, clientes, procesos internos, aprendizaje y desarrollo―y (2) concebirse en función de cuatro grupos de mapas estratégicos: mapas de las operaciones TI (1), mapas de los proyectos TI (2), mapas conformados a partir del tributo de los grupos de mapas 1 y 2 conformando los mapas de las TI estratégicas (3) y, finalmente, la integración de estos 3 grupos con el clásico mapa estratégico a nivel organizacional (4). La integración de estos cuatro grupos de mapas se denomina *BSC en cascada* [Kaplan and Norton, 2004; citados por López Paz]. El proceso de construir el IT BSC es, esencialmente, un proceso colaborativo de definición de la *tríada* perspectiva/ objetivos/indicador.

El BSC de TI es uno de los más eficaces medios de ayuda a la junta y a la dirección para lograr la alineación del negocio y TI. Los objetivos son determinar un medio para que la dirección informe a la junta; promueva el consenso entre los objetivos estratégicos de TI; demuestre la eficacia y añada el valor de TI; y se comunique sobre el rendimiento, los riesgos y las capacidades de las TI [ITGI, 2007].

1.3.5. Objetivos de Control para Tecnología de Información (COBIT, Control Objectives for Information and related Technology)

COBIT es una herramienta de las TI, lanzada inicialmente en 1996, que ha cambiado la forma en que trabajan los profesionales de TI. Vinculando tecnología informática y prácticas de control, consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores. Es una base mundialmente aceptada para el gobierno de TI sobre la base de los estándares de la

industria y las buenas prácticas. Una vez implementado, los ejecutivos pueden asegurar que la TI es alineada eficazmente con los objetivos de la empresa y pueden dirigir mejor el uso de TI para la ventaja de la empresa. Provee un lenguaje común a todos los ejecutivos para comunicar objetivos de TI, y los objetivos y resultados de las auditorías [ITGI & OGC, 2008].

A continuación se relacionan algunos elementos que describen y caracterizan a COBIT.

Misión: Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores

Características:

- Orientado al negocio
- Alineado con estándares y regulaciones "de facto"
- Basado en una revisión crítica y analítica de las tareas y actividades en TI
- Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA)

Los beneficios de implementar COBIT como marco de referencia para la gestión de las TI incluyen: mejor alineación, con base en su enfoque de negocios; una visión, entendible para la gerencia, de lo que hace TI; propiedad y responsabilidades claras, con base en su orientación a procesos; aceptación general de terceros y reguladores; y entendimiento compartido entre todos los participantes, con base en un lenguaje común.

El marco de trabajo de COBIT (figura 1.2) se basa en el principio de proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de información [COBIT4.1, 2007].

El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro “dominios” principales, a saber: Planificación y organización, Adquisición e implantación, Entrega y soporte y Monitoreo y evaluación. Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda, facilitando que la generación y

procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y con fiabilidad.

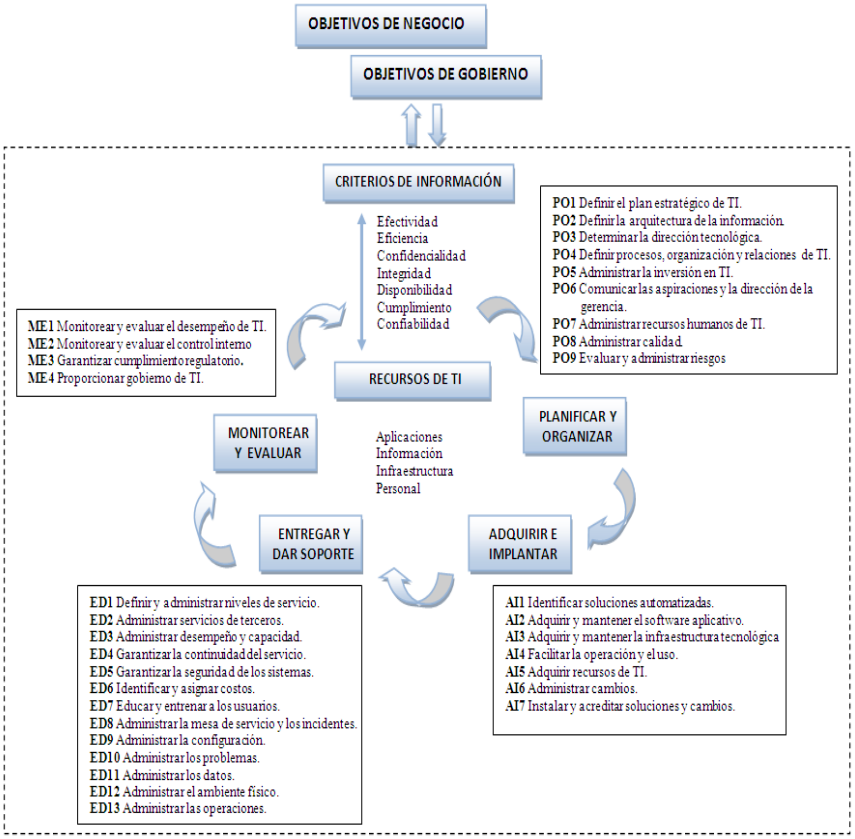


Figura 1.2. Marco de trabajo general de COBIT [Fuente: COBIT4.1, 2007].

Asimismo, se deben tomar en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano. Cualquier tipo de empresa puede adoptar una metodología COBIT, como parte de un proceso de reingeniería en aras de reducir los índices de incertidumbre sobre vulnerabilidades y riesgos de los recursos TI y consecuentemente, sobre la posibilidad de evaluar el logro de los objetivos del negocio apalancado en procesos tecnológicos.

1.4. Alineación de la TI al negocio

Por casi tres décadas, profesionistas, académicos, consultores y departamentos de investigación han identificado la carencia de alineación TI/Organización como una preocupación fundamental de las organizaciones y un problema considerable. Debido a la gran dependencia de los procesos del negocio con la tecnología, tanto los líderes de TI

como del negocio se encuentran buscando continuamente prácticas gerenciales que los ayude a alinear las estrategias de TI con la organización [Corona, 2010].

Explica el autor que la alineación estratégica se enfoca en las actividades que la gerencia lleva a cabo para lograr una cohesión en los objetivos a través del departamento de TI y otros departamentos funcionales de la organización (ej. Finanzas, Mercadotecnia, HHRR, Manufactura). Por lo tanto, la alineación debe cumplir con ambas perspectivas, cómo TI está en armonía con la organización, y como la organización debería, o podría estar en armonía con TI.

Los esfuerzos para integrar las TI con el negocio se condensan en un área temática denominada *alineación de las TI con el negocio* (Business IT Alignment). La condición de alinear las TI se está convirtiendo más que en una posibilidad en una imperiosa necesidad [López Paz, 2009].

Henderson y Venkatraman en fueron los primeros que describieron claramente la interrelación entre las estrategias de negocio y las estrategias de TI en su conocido Modelo de Alineamiento Estratégico (SAM, Strategic Alignment Model). El concepto del SAM está basado en dos bloques: el " Ajuste estratégico" y la " Integración funcional." El ajuste estratégico reconoce que la estrategia de TI debe ser articulada en relación con un dominio externo (cómo la firma es colocada en el mercado de TI) y un dominio interno (cómo la infraestructura de TI debe ser arreglada y dirigida). El ajuste estratégico es por supuesto equitativamente relevante en el dominio de la empresa. Dos tipos de la integración funcional existen: integración estratégica e integración de operaciones. La integración estratégica es el enlace entre la estrategia de la empresa y la estrategia de TI que debe reflejar los componentes externos, lo que es importante para muchas compañías ya que es el un origen de una ventaja estratégica. La integración de operaciones cubre el dominio interno y se las arregla con el enlace entre infraestructura organizativa, los procesos y la infraestructura de TI para suministrar a profesionales la orientación práctica en la alianza de la empresa / TI.

Argumentan que los dominios externo e interno son igualmente importantes, pero los directivos tradicionales piensan en la estrategia de TI en términos del dominio interno, ya que históricamente TI fue vista como una función de soporte que era poco esencial para el

negocio. En sus resultados de investigación Henderson y Venkatraman alertan sobre los problemas que pueden aflorar cuando es considerado un enfoque bivariado con respecto al equilibrio de los cuatro dominios (estrategia de TI, estrategia de negocio, infraestructura de SI e infraestructura organizacional). Por ejemplo, cuando solo los elementos externos (estrategia de TI, estrategia de negocio) son considerados, una seria subestimación de la importancia de los elementos internos, como el rediseño requerido de los procesos claves de negocio, puede ocurrir [Van Grembergen, & De Haes, 2009].

Según Sarah Meyer (2007) la infraestructura de TI, para alinear sus actividades con los objetivos empresariales, necesita optimizar los servicios según las prioridades empresariales y el éxito de los usuarios. Entre las ventajas se incluyen mejores servicios y costes reducidos, además del establecimiento de la infraestructura de TI como un proveedor de servicios estratégicos que puede aportar valor a su empresa. El primer paso clave hacia la alineación empresarial es la adopción de un enfoque centrado en procesos para la gestión de TI.

En una economía como la actual, las organizaciones están demandando a sus gerencias de TI que hagan inversiones "sabias" y que puedan demostrar su valor para el negocio. Dicha demanda ha traído un concepto denominado como *Business Service Management* (BSM) el cual se considera como el vínculo ideal entre los servicios de TI y las necesidades del negocio. Por ello se dice que BSM es una estrategia proactiva de la gestión de TI que permite a las organizaciones alinear sus recursos de TI con sus prioridades de negocios e incluso, a nivel operativo, detectar los problemas en los servicios de TI antes que impacten al usuario final del negocio [Espìnosa, G].

En la práctica, las organizaciones a menudo tratan de expresar un número de "principios de alineación negocio/TI". Algunos ejemplo de principios usados en organizaciones de la vida real son señalados por Van Grembergen et al., (2009).

Para evaluar la alineación se han desarrollado algunas propuestas. Entre estas Weill & Broadbent [1998 citado por Van Grembergen et al., 2009] propone un indicador basado en la calificación de una grupo de preguntas sencillas. Posteriormente Weill & Ross [2004 citado por Van Grembergen et al., 2009] proponen un "indicador de desempeño de gobierno". Se basa en la puntuación asignada a resultados percibidos de gobierno, en una

escala de 1 (no importante) a 5 (muy importante). Se deben calificar en base a dos preguntas, cuán importante es el resultado específico de gobierno y cuán bien el gobierno de TI contribuyó a alcanzar el resultado. Basado en las puntuaciones es calculado el indicador. Las respuestas de la primera pregunta son usadas para pesar las respuestas de la segunda. También se pueden encontrar algunos modelos de madures de alineación. Ejemplo de estos modelos de madurez fueron desarrollados por Luftman (2000) y Duffy (2002). Luftman define cinco niveles, a través de la definición de un conjunto de criterios, compuestos por una variedad de atributos. Duffy define cuatro niveles, donde en el primero hay una desconexión entre los ejecutivos de tecnología y el resto de la administración corporativa; y el nivel cuatro implica que TI y el negocio están entrelazados inseparablemente y existe solo una estrategia que incorpora ambos.

1.5. Gestión de riesgos

Las TI tienen un papel esencial en el mundo de los negocios de hoy. Los incidentes cruciales en TI afectan los procesos de las empresas considerablemente y pueden resultar en la pérdida de ingreso y daño de ideas. La relevancia creciente de TI cambia de lugar los riesgos de TI, su detección y el manejo del enfoque de los responsables de TI. Además los requisitos legales y reguladores para la prevención de riesgos de operaciones están creciendo, exigiendo la prevención de riesgos con un sistema de alerta avanzada.

Según De Oro Gómez (2010) la medida del riesgo, la evaluación y selección de opciones para mitigarlo, gestionando las amenazas que pueden afectar al éxito del negocio, es una disciplina por todos conocida como gestión del riesgo. Sin embargo, la propia definición de riesgo puede variar sustancialmente según la experiencia y formación de cada profesional o del contexto dentro de la organización.

La ISO define el riesgo de TI como: “La potencialidad de que una amenaza determinada aproveche las vulnerabilidades de un activo o grupo de activos y por lo tanto pueda causar daño a la organización. Se mide en términos de una combinación de la probabilidad de un suceso y sus consecuencias” [ISO/IEC 13335-1: 2007].

De manera similar El Instituto Nacional de Estándares y Tecnología de EU, plantea que: “El riesgo relacionado a las TI, considera: (1) la probabilidad de que una fuente de amenaza en particular actúe (intencional o accidentalmente) sobre la vulnerabilidad de un sistema de

información en particular y (2) el impacto resultante si esto ocurriera" [NIST 800-30: 2002].

El concepto de riesgo de TI puede definirse como el efecto de una causa multiplicado por la frecuencia probable de ocurrencia dentro del entorno de TI. Surge así, entonces la necesidad del control que actúe sobre la causa del riesgo para minimizar sus efectos. Cuando se dice que los controles minimizan los riesgos, lo que en verdad hacen es actuar sobre las causas de los riesgos, para minimizar sus efectos [Maxitana Cevallos, 2005].

El Framework de Riesgos de TI (2009) categoriza los riesgos de TI de tres modos: *Riesgos de entrega de servicios de TI, Riesgos de entrega / beneficio en la realización de soluciones de TI* y *Riesgos de beneficio de realización de TI*.

La empresa Symantec, una de las más importantes empresas de seguridad de la información, en su Reporte de Gestión de Riesgos de TI [IT Risk Management Report Volumen 2: 2008] diferencia cuatro clases de elementos de Riesgos de TI, acorde a sus fuentes e impacto potencial en la organización, específicamente:

- *Riesgos de seguridad*, la información puede ser accedida, manipulada o usada por partes no autorizadas.
- *Riesgos de disponibilidad*, la información o aplicaciones pueden hacerse inaccesibles por fallos de procesos, personas o sistemas, o desastres naturales.
- *Riesgos de desempeño*, el bajo desempeño de sistemas, aplicaciones, personal u organizaciones puede disminuir el valor o productividad del negocio.
- *Riesgos de conformidad*, la información manipulada o procesada puede no cumplir las regulaciones apropiadas, principios de requerimientos de TI o del negocio.

En la tabla 1.1 se muestra información adicional y ejemplos de fuentes, impactos potenciales de los riesgos en cada una de las categorías y los valores fundamentales que se comprometen en la empresa.

Tabla 1.1. Riesgos de TI: Fuente, impacto potencial y valores fundamentales comprometidos.

CATEGORÍA DE RIESGO	FUENTE	IMPACTO POTENCIAL	VALORES COMPROMETIDOS
Seguridad ***Compromiso de la información, confianza en esta y tecnologías y procesos para su gestión.***	- Ataques externos - Códigos malignos - Destrucción física - Accesos inapropiados - Empleados descontentos - Proliferación de plataformas y tipos de mensajería	- Corrupción de la información - Fraudes externos - Robo de identidad - Robo de activos financieros - Daño a la reputación y marca - Daño a los activos	- Confianza - Reputación de los clientes
Disponibilidad ***Fallo o demora en la entrega de los procesos de TI o de informaciones necesarias para las transacciones comerciales y las operaciones.***	- Fallo de hardware - Interrupción de redes - Gestión inadecuada de los cambios - Fallos de los data centers - Desastres regionales - De fuerza mayor	- Transacciones abandonadas y pérdida de ventas - Reducción de la confianza de clientes, socios y empleados - Interrupción o demora de los procesos críticos de negocio. - Disminución de la productividad del personal de TI	- Financieros - De Integridad de la cadena de suministro - Responsabilidad comercial
Desempeño ***Operación lenta o ineficiente de los procesos de TI que soportan las transacciones y operaciones del negocio***	- Pobre arquitectura de los sistemas - Congestión de redes - Código ineficiente - Inadecuada capacidad - Inefectivo diseño de procesos.	- Reducción de la satisfacción de los clientes - Reducción de la lealtad de los clientes o socios - Reducción de la productividad de los usuarios - Interrupción o demora de los procesos críticos de negocio - Pérdida de la productividad de TI	- Eficiencia - Productividad
Conformidad ***Penalizaciones, multas y pérdida de reputación por fallos en el cumplimiento de leyes y regulaciones, o consecuencias de no conformidad con las políticas de TI***	- Regulaciones alteradas o malentendidas - Acciones legales - Métodos de protección internos de TI para apoyar la conformidad - Estándares de conformidad, de terceros, inadecuados - Insuficientes capacidades de auditoría. - Políticas de TI ausentes o mal definidas	- Daños a la reputación - Brechas en la confidencialidad de los clientes - Litigaciones	- Integridad legal - Integridad financiera - Integridad operacional

[Fuente: Elaboración propia a partir de IT Risk Management Report Volumen 2, 2008].

En un concepto más amplio acerca de la gestión de riesgos la guía de administración de riesgos del Instituto Nacional de Estándares y Tecnología de EU lo define como: el proceso de identificar, controlar y mitigar los riesgos relacionados con los sistemas de información. Este incluye la estimación de riesgos, análisis costo beneficio; y selección, implementación, prueba y evaluación de la seguridad de medidas. Este sistema completo de revisión de la seguridad considera tanto la eficiencia como la efectividad, incluyendo el impacto en la misión y las restricciones debido a políticas, regulaciones y leyes. [NIST 800-30: 2002]

Utilizando el lenguaje adecuado para hablar de riesgos y disponiendo de los instrumentos adecuados para gestionarlos, las empresas pueden obtener un valor añadido, además de evitar los riesgos. Pueden servirse de la gestión de riesgos para introducir cambios que también generan mayor eficacia de TI y agilidad en el entorno corporativo en general. El hecho es que la gestión de riesgos de TI no es una cuestión técnica. Es de gestión. La eficacia en este ámbito se consigue mejorando el modo de gestionar TI. [IBM, 2009]

1.6. Evaluación de la GTI

La evaluación de desempeño es la forma reconocida que compara la posición actual con las metas predeterminadas o usadas para la planeación y selección de objetivos. Por lo tanto estos primeros pasos en la implementación de gobierno de TI en las organizaciones son reconocidos, lo cual es la base de una correcta planeación. El reconocimiento de la situación presente puede ayudar a encontrar fortalezas y debilidades. Esto también ayuda a ofrecer planes para el desarrollo de gobierno de TI [Borousan, E. et al., 2011].

Sánchez Hilara (2008) define un conjunto de categorías de indicadores para evaluar la calidad de los servicios de TI, que incluyen: indicadores tecnológicos, indicadores de actividad funcional, indicadores de proceso, indicadores departamentales, indicadores de servicio, indicadores de ventana de servicio y los indicadores de contexto.

Lo más referido a evaluación de gestión de TI está relacionado con las Auditorías de TI. Existen numerosas empresas internacionales que brindan servicios de consultoría en este sentido, pero por supuesto no es público el *cómo* lo hacen y además son servicios extremadamente caros. Dentro de los modelos "públicos" de auditoría se destacan las Directrices de Auditoría propuestas por COBIT, cuyo propósito es contar con una estructura sencilla para auditar y evaluar controles, con base en prácticas de auditoría

generalmente aceptada y compatible con su esquema global. Estas directrices de auditoría proporcionan guías para preparar planes de auditoría que se integran al framework de COBIT. Sin embargo, las directrices no son exhaustivas ni definitivas. No pueden incluir todo ni ser aplicables a todo, así que deberán ajustarse a condiciones específicas [Colectivo, 2008].

La función de las auditorías de TI es básicamente una función de soporte para el logro convencional de sus objetivos. Las auditorías de TI son el proceso de coleccionar y valorar las pruebas, para determinar si un sistema de información protege la ventaja, mantiene la integridad de datos, alcanza los objetivos organizacionales eficazmente, y consume los recursos eficientemente. Dos de sus objetivos principales son averiguar la extensión del acatamiento con las políticas, los planes y los procedimientos de la organización y determinar la eficacia y la eficiencia de la información, los equipos y el software en la organización [Pathak, 2005].

1.7. Experiencias en el mundo y Cuba

La gobernabilidad de las TI se ha convertido en un tema importante, debido al impacto del mismo sobre las organizaciones. Para el año 2008 el porcentaje de organizaciones que estaban inmersas en el proceso de implementar o ya habían implementado prácticas de gobierno de TI en las diferentes regiones eran: Latinoamérica, 27%; Asia, 44%; Europa, 50% y Norteamérica, 50% [Gómez, 2008].

El estudio aplicado por el ITGI en el 2008 a diferentes organizaciones de todo el mundo reflejó que la importancia de TI sigue creciendo y ha aumentado significativamente el interés por la adopción y uso de las mejores prácticas, pero persisten aún muchos incidentes relativos a TI. Aunque la seguridad y la conformidad constituyen elementos importantes señalados, las personas son el problema más crítico.

Los estudios actuales sobre el control de gestión de las TI en los departamentos TI reconocen, como una de las principales limitantes, que éstos no han ofrecido un verdadero control orientado a servicios. En su lugar reflejan detalles limitados de cómo controlar y localizar los costos de los departamentos de servicios basados en técnicas de reducción de costos [S. Son, 2006 citado por López Paz, 2009].

En América Latina existe un pobre desarrollo en cuanto a implantación de modelos, estándares y buenas prácticas que permitan gestionar las TI, no tan fuerte como el que se puede apreciar en la India, EUA y Reino Unido entre otros. Aunque algunos países, ya han comenzado a pronunciarse por la importancia de la gestión de TI; la Contraloría General de la República de Costa Rica (CGR) emitió una normativa en la temática de las TI cuyo propósito es orientar el fortalecimiento de la gestión de TI.

La investigación de las prácticas de GTI en cientos de compañías en todo el mundo ha revelado que la mayoría de las organizaciones no están optimizando su inversión en TI. Cuba no escapa de este fenómeno, la pobre gestión de los servicios de TI en las empresas del país atentan contra el retorno de la inversión de las mismas. El factor diferenciador entre los que lo consiguen y los que no, radica en la participación de la dirección en las decisiones clave de TI. La correcta participación de la dirección en dichas decisiones aporta un valor real a la inversión en TI.

En enero del 2000 se crea el Ministerio de Informática y las Comunicaciones (MIC) en nuestro país. Una de sus prioridades es revitalizar y actualizar la estrategia de la informatización de la sociedad cubana y las funciones ramales. Sin embargo este ministerio no se ha pronunciado explícitamente por la gestión de las TI en función de los objetivos del negocio en el sector empresarial y se enfoca principalmente en aspectos relativos a la seguridad de la información y las redes. Por otra parte en el Decreto No. 281 "Reglamento para la implantación y consolidación del sistema de dirección y gestión empresarial estatal" se plantea en el Artículo 583 que "Los recursos de la tecnología de información deben ser controlados con el objetivo de garantizar el cumplimiento de los requisitos del sistema de información que la empresa necesita para el logro de su misión." En el año 2009 se aprobó la Ley No. 107 "Ley de la Contraloría General de la República de Cuba", y en este mismo año se emite una guía de autocontrol del sistema de control interno, en la cual se incluyen aspectos relativos a verificar al control de la tecnología de información como son: la existencia de un plan de seguridad informática, la seguridad de los sistemas contables-financieros, los mecanismos para el control y supervisión de los medios de computación, entre otros; en todos los casos referidos a la seguridad pero no al aporte real de TI a los objetivos empresariales.

Las empresas cubanas reconocen la importancia de las TI y su gestión, sin embargo, continúan existiendo algunas concepciones erróneas en torno a esto, pues ha existido un uso inadecuado de las mismas sin el logro de los resultados esperados, creándose así limitaciones en su uso. Muchas cuentan con recursos que no son explotados en toda su magnitud en función de las necesidades de su negocio, entre las principales causas se puede mencionar que la gestión no ha sido lo suficientemente acertada, pues la inversión en TI no garantiza su éxito, hay que saberlas utilizar para poder hacer un correcto uso de las mismas, a través de buena gestión. Debido al desconocimiento, en estos momentos existen quienes niegan su empleo pues no calculan la verdadera magnitud de sus beneficios. Algunas organizaciones llevan ventaja en cuanto al manejo de las TI, tales como ETECSA, CIMEX, DATYS, DESOFT, COPEXTEL, MINBAS (Empresa Eléctrica), Banco Nacional de Cuba (BNC); que, aunque todavía no se han planteado una verdadera gestión de las TI, han realizado algunos esfuerzos en este sentido.

Es de destacar un estudio realizado en el 2008 por la empresa CIMEX [Gómez, 2008]. Entre los resultados arrojados sobre el nivel de conocimiento que los ejecutivos tienen acerca del proceso de Gestión de las TI en estas empresas.

- Un 47% de los encuestados esperan que la gobernabilidad de las tecnologías de la información sea un éxito en la empresa y que de manera efectiva colabore con el alcance de los objetivos estratégicos, asegurar mejoras en la eficiencia, asegurar que la información crítica para el negocio está disponible cuando se necesita, que sea confiable y confidencial.
- Se denotó que es necesario concientizar acerca del grado de importancia que la empresa debe prestar a las TI, ya que cerca de dos tercios (65% de los consultados) indicaron que solo a veces son tratadas las TI en las reuniones del consejo, dando al traste también con la falta de alineación existente en las TI en la empresa como consecuencia de la falta de un programa de gobernabilidad de TI.
- La seguridad de la información resultó ser el asunto que más les preocupa a los ejecutivos, identificándola el 48% de los encuestados como su principal prioridad.

1.8. Conclusiones parciales

1. El análisis del estado del arte evidencia aun más la importancia de las TI en el desarrollo del ámbito empresarial, así como la necesidad de gestionarlas para alinear sus objetivos con los de las empresas y obtener resultados que resulten en ventajas competitivas.
2. La gestión de TI para que sea efectiva debe abarcar la gestión de los riesgos, la mejora de los servicios y la alineación de las inversiones de TI con el negocio.
3. Las inversiones en TI por sí solas no garantizan el éxito organizacional, éstas se deben basar en una adecuada gestión de TI que permita alinear los objetivos de las TI con los del negocio, por ende los estudios de dicha gestión son necesarios en aquellas empresas que deseen mejorar continuamente.
4. El análisis del estado de la práctica demuestra la necesidad de elevar el número de herramientas que permitan la evaluación y mejora de la GTI en las organizaciones, con el propósito de que las TI garanticen las metas organizacionales tanto en Cuba como en el mundo.

Capítulo 2. Procedimiento para diagnosticar la gestión de TI

El análisis del estado del arte y de la práctica plasmado en el marco teórico-referencial que sustenta esta investigación evidenció la necesidad de aplicar un procedimiento para diagnosticar el estado actual de la gestión de Tecnologías de la Información (TI) en las empresas ATI y TECNOAZUCAR VC. En este capítulo se describen brevemente cada una de las etapas y pasos en que está dividido el procedimiento seleccionado, y se relaciona la caracterización de las empresas objeto de estudio.

2.1. Procedimiento para diagnosticar el estado actual de la gestión de TI

El procedimiento está estructurado en 8 etapas como se muestra en la figura 2.1 y tiene como *objetivo*: evaluar la gestión de TI en una organización, considerando la alineación de TI a los objetivos de negocio y la administración de los riesgos y beneficios asociados.

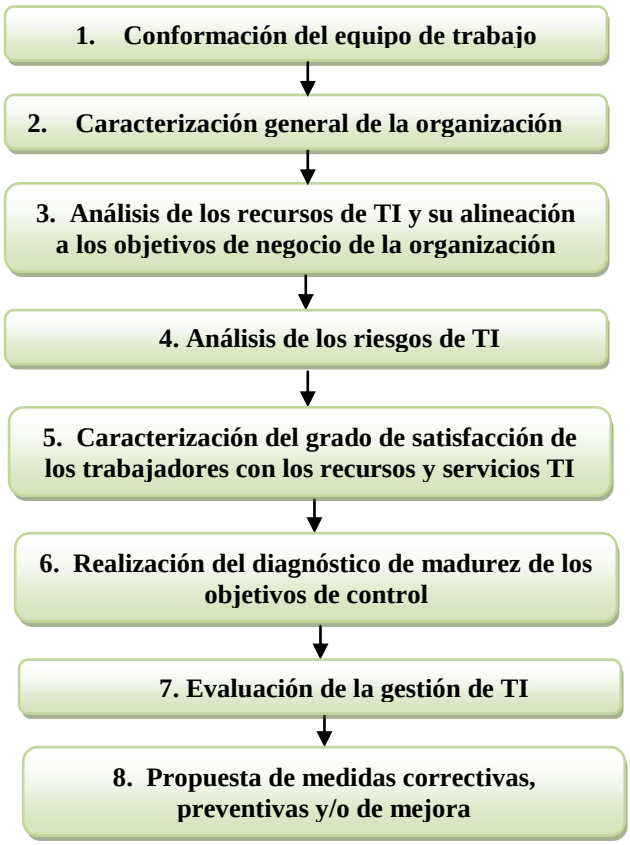


Figura 2.1. Procedimiento para diagnosticar el estado actual de la gestión de TI (Pérez Lorences, 2010**)**

El procedimiento se inicia en la primera etapa con la conformación del equipo de trabajo y en la segunda etapa se procede a realizar la caracterización general de la organización que se haya seleccionado para aplicar el diagnóstico. La tercera etapa está dedicada a analizar la alineación de los recursos de TI a los objetivos de negocio de la organización, proponiéndose un conjunto de herramientas para llevar a cabo esta valoración. En la cuarta etapa se propone un procedimiento específico para analizar la administración de los riesgos de TI que permite además obtener una valoración de los riesgos en la organización. Por su importancia como reflejo de las acciones de la gestión de TI en la etapa cinco se caracteriza el grado de satisfacción de los trabajadores con los recursos y servicios de TI. La realización del diagnóstico de madurez se efectúa en la sexta etapa y posteriormente se evalúa la gestión de TI utilizando la propuesta de cálculo de un indicador integral de gestión de TI que caracteriza el estado actual de la organización al respecto. El procedimiento culmina con la propuesta de medidas correctivas, preventivas y/o de mejora, en función de la evaluación efectuada, creando las bases para la mejora continua de la gestión de TI en la organización. A continuación se explican brevemente las etapas y pasos del procedimiento:

Etapa 1: Conformación del equipo de trabajo

La primera etapa está dirigida a la conformación del equipo de trabajo, el cual tendrá como función la aplicación completa del procedimiento. Incluye: 1.1 *Definir estructura del equipo de trabajo,* 1.2 *Determinar cantidad de miembros y seleccionar el personal,* 1.3 *Asignación de responsabilidades y tareas a realizar,* 1.4 *Capacitación del equipo de trabajo.*

Etapa 2: Caracterización general de la organización objeto de estudio

Esta segunda etapa corresponde a la caracterización general de la organización objeto de estudio, y debe comenzarse a apreciar el valor de las tecnologías de información para el logro de los objetivos de su negocio. Esta etapa requiere considerar aspectos formales para orientar el estudio a realizar posteriormente y se distribuye en los dos pasos siguientes: 2.1 *Describir los datos generales de la organización* y 2.2 *Identificar los objetivos y procesos del negocio.*

Etapa 3: Análisis de los recursos de TI y su alineación a los objetivos de negocio de la organización

En esta etapa se analizará el impacto de TI en el logro de los objetivos de negocio y las condiciones actuales de la empresa para satisfacer estos requerimientos. Esta etapa se desagrega en los pasos siguientes:

3.1. *Efectuar un inventario de los recursos de TI de la organización*

Deben identificarse: las aplicaciones, la infraestructura, y el personal. Para llevar a cabo el inventario se propone que el registro de la información sea apoyado con el modelo mostrado en la tabla 2.1. La clasificación del recurso en función de su impacto en el negocio será asignada al concluir el paso 3.2.

Tabla 2.1. Modelo de inventario para los recursos de TI

No	Recurso	Clasificación			Descripción breve	Proceso(s) relacionado(s)	Impacto		
		Aplicación	Infraestructura	Personal			Fuerte	Medio	Débil

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 organización se procede a efectuar la clasificación de éstos en función de su impacto en el negocio, que puede apoyarse en el algoritmo de la figura 2.2.

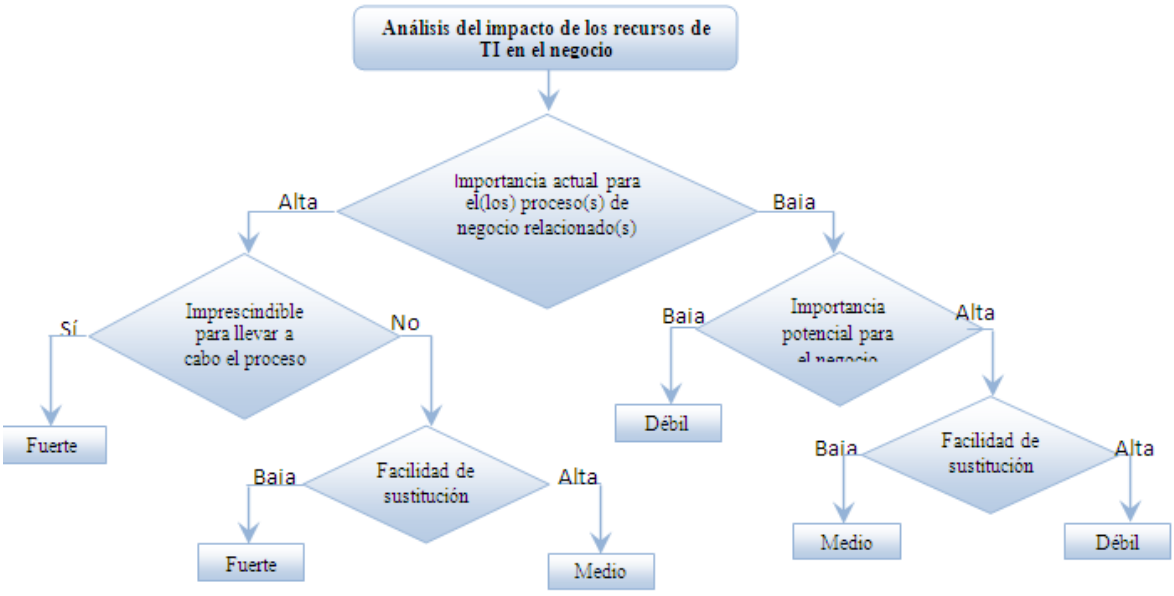


Figura 2.2. Algoritmo para la clasificación de los recursos de TI en función de su impacto en el negocio

El mayor índice de cada tipo de recurso determinará su clasificación, lo que permitirá valorar que tipo de recurso impacta en mayor medida en el negocio.

$$IRR_{ij} = \frac{\sum_{1}^{m} NC_{ji}}{\sum_{1}^{n} NR_i} \times 100 \qquad (2.1)$$

Donde:

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

$\sum_{1}^{m} NC_{ji}$: Valor total de clasificaciones "j" del recurso tipo "i".

$\sum_{1}^{n} NR_i$: 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 TI en el negocio de la organización objeto de estudio se propone el índice relativo global calculado mediante la expresión 2.2:

$$IRTI_{j} = \frac{\sum_{1}^{m} NC_{j}}{\sum_{1}^{n} NRTI} \times 100 \qquad (2.2)$$

Donde:

$IRTI_j$: Índice relativo global de los recursos de TI según clasificación "j"

$\sum_{1}^{m} NC_{j}$: Valor total de clasificaciones "j"

$\sum_{1}^{n} NRTI$: Valor total de recursos de 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 TI en el negocio es Fuerte, Medio o Débil.

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

A partir de los elementos consultados y la valoración práctica de algunas empresas, se decidió para llevar a cabo la evaluación de los procesos de negocio; definir el grado de dependencia de TI en tres niveles, de la forma siguiente:

Fuerte: TI debe ser parte de la estrategia de negocio de la organización. La existencia de las TI determina totalmente la ejecución de los procesos de negocio. Son indispensables para obtener el producto o servicio brindado. Las TI están enfocadas en el cliente, los clientes de la organización son clientes de TI.

Medio: Las TI pueden convertirse en un elemento diferenciador para los resultados obtenidos por el negocio, aumentado la calidad y efectividad del producto o servicio brindado. Pueden utilizarse en un gran número de actividades, y su interrupción o ausencia dificulta el alcance de los objetivos. Las TI añaden valor en el proceso de negocio, y son enfocadas en productos y servicios que sirven de apoyo.

Débil: las TI pueden facilitar la ejecución de los procesos de negocio, apoyando la realización de algunas actividades, pero su interrupción no imposibilita el logro de los objetivos planteados. Las TI son enfocadas en los componentes de tecnología.

3.4. *Analizar la correspondencia entre los recursos de TI y los requerimientos de la organización 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 de negocio en función de su grado de dependencia de TI, en este paso se procede a analizar la alineación entre ambos aspectos para diagnosticar la situación actual de la organización al respecto. Para apoyar este análisis se desarrolló en esta investigación la matriz que se muestra en la figura 2.3.

Impacto de los recursos de TI

Dependencia de los procesos de negocio	**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*

Figura 2.3. Matriz dependencia de procesos de negocio / impacto de recursos de TI, análisis de alineación

La matriz resulta útil para analizar la alineación y posibles estrategias a seguir. Para los casos en que, tanto la dependencia de los procesos como el impacto de los recursos fueran fuertes, existe una alineación adecuada para satisfacer los requerimientos de la organización, debe continuar potenciándose la gestión de estos recursos en beneficio del negocio. Si el impacto de los recursos es fuerte y la dependencia media e incluso débil, entonces no existe alineación adecuada; deben identificarse las oportunidades que ofrece TI y valorar cómo los procesos de negocio pueden aprovechar estas potencialidades. La clasificación en medio y débil de los recursos de TI siendo fuerte la dependencia de los procesos refleja que los recursos de TI no logran satisfacer plenamente las necesidades del negocio y debe analizarse su uso actual y valorar proyectos de inversión en TI, de manera similar bajo un impacto débil es necesaria la adquisición de recursos en función de los requerimientos. Si es débil en ambos casos, puede clasificarse como alineación pero se propone realizar mejoras de proceso e identificar cómo TI puede apoyar al negocio.

Etapa 4: Análisis de los riesgos de TI y su administración

En esta etapa se procede a analizar la administración de los riesgos de TI en la empresa. Para esto se emplea el procedimiento específico (figura 2.4), que permite obtener una valoración de los riesgos de TI, e incluye en cada paso la pregunta clave a responder para analizar cómo se lleva a cabo su administración. El contenido de cada paso, por una parte guía la ejecución del diagnóstico para obtener los riesgos, y por la otra brinda los elementos necesarios para dar respuesta a la pregunta planteada, posibilitando el análisis de su administración.

1. *Establecer el contexto estratégico de riesgos*

- ¿Están identificados los recursos críticos de TI?

Es necesario primeramente establecer el alcance de la gestión de riesgos de TI dentro de la organización e identificar los recursos críticos de TI. A partir de la clasificación realizada en la etapa anterior, es posible determinar de los recursos que fueron clasificados como impacto Fuerte sobre los objetivos del negocio, cuáles son críticos, en función de establecer niveles de prioridad en el análisis posterior. La criticidad de los recursos de TI puede también estar basada en el nivel de protección que se requiere para mantener la disponibilidad, confidencialidad e integridad de los mismos. Es importante señalar que los

dueños de los sistemas de TI son los responsables de determinar el nivel de impacto sobre sus sistemas y la información asociada, por tanto este análisis debe complementarse con entrevistas a dicho personal.

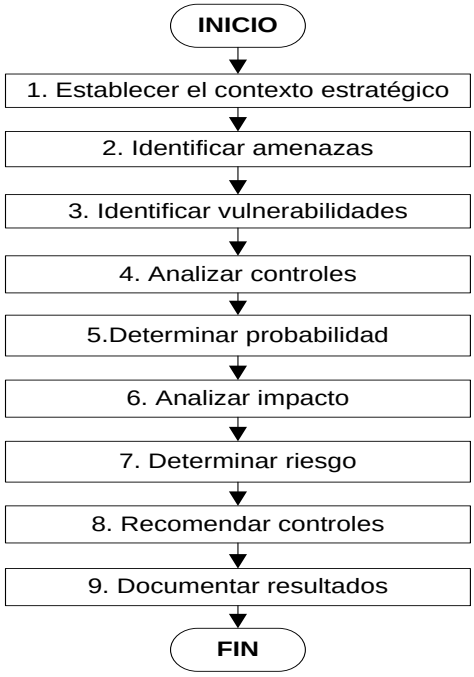


Figura 2.4. Procedimiento específico para la valoración del riesgo de TI

2. *Identificar amenaza*

- ¿Están identificadas las amenazas?

El objetivo de este paso es determinar las fuentes potenciales de amenazas. Deben revisarse los historiales de reportes de violación de la seguridad de los sistemas, reportes de incidentes, etc.; además de entrevistar al personal de TI de la organización y a los usuarios. Comúnmente las amenazas se clasifican en tres tipos [NIST 800-30: 2002]:

-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, ya sean actos no intencionales o acciones deliberadas.

Es importante considerar además las amenazas desde el punto de vista interno o externo que puedan ocasionar riesgos de conformidad y/o desempeño.

3. *Identificar vulnerabilidades*

- ¿Están identificadas las vulnerabilidades?

Es necesario identificar el listado de vulnerabilidades de TI, técnicas o no, incluyendo las relativas al personal, que pueden ser explotadas por las fuentes de amenazas. Basado en los aspectos señalados en la norma NIST 800-30: 2002, se recomienda para identificar las vulnerabilidades:

-el uso de fuentes reconocidas de vulnerabilidades: por ejemplo publicadas en la web por vendedores de los sistemas y otras empresas.

-la prueba del desempeño de la seguridad de los sistemas: pueden ser usadas herramientas automáticas de escaneo de vulnerabilidades y poner a prueba la efectividad de los controles de seguridad que están siendo aplicados.

-el desarrollo de listas de chequeo de requerimientos de seguridad: considerando elementos técnicos, operacionales y de gestión.

4. *Analizar controles*

- ¿Qué controles están implementados?

En este paso se procede a analizar los controles que han sido implementados, o planeados para implementarse en la organización; para minimizar o eliminar la probabilidad de que las amenazas actúen sobre las vulnerabilidades. Este análisis se realiza porque para estimar la probabilidad de que una amenaza actúe sobre una vulnerabilidad es necesario considerar los controles que se han implementado o planeado, que pueden reducir estas posibilidades.

Los controles pueden ser técnicos o no. Los técnicos son incorporados al hardware o software (ej. mecanismos de control de accesos, mecanismos de identificación y autentificación, métodos de encriptación, software de detección de intrusos y otros). Los no técnicos son controles operacionales y de gestión, como políticas de seguridad, procedimientos operacionales y medidas de seguridad de personal, instalaciones físicas y el medioambiente. Para ambos casos los controles pueden ser preventivos o de detección. Los

controles preventivos inhiben los intentos de violar políticas de seguridad y los de detección advierten sobre la violación o intento de violar las políticas se seguridad.

En el análisis de los controles, de manera similar al paso anterior, la creación de una lista de chequeo puede ser útil para apoyar el análisis de manera sistemática, pero es esencial la actualización periódica de este instrumento para garantizar su validez. El resultado de este paso es una lista de los controles existentes o planeados y el análisis de su efectividad.

5. *Determinar nivel de probabilidad*

- ¿Están determinadas las probabilidades de que una amenaza actúe sobre una vulnerabilidad, considerando los controles existentes?

Para determinar la probabilidad de ocurrencia debe considerarse el resultado de los pasos anteriores, o sea, las fuentes de amenazas, las vulnerabilidades, y la existencia y efectividad de controles. Esta probabilidad generalmente es descrita en niveles más o menos profundos. En esta investigación se propone el uso de la escala: Alto, Medio y Bajo para clasificar el nivel de probabilidad; considerada a partir del análisis de los tres factores mencionados anteriormente. La tabla 2.2 muestra la propuesta realizada.

Tabla 2.2. Escala de nivel de probabilidad para la valoración del riesgo de TI

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.

6. *Analizar impacto*

- ¿Se han analizado los impactos de que una amenaza actúe sobre una vulnerabilidad?

Otro paso importante para la valoración de los riesgos es determinar el impacto negativo sobre el negocio, de que una amenaza actué exitosamente sobre una vulnerabilidad. Este análisis parte de la identificación de recursos críticos realizada en el primer paso.

El impacto puede ser descrito en términos de pérdida o degradación de alguno, o la combinación de algunos, de los cuatro elementos de riesgos ya descritos en el Capítulo1, que son: seguridad, disponibilidad, desempeño y conformidad. Algunos impactos tangibles

pueden ser medidos en términos de pérdida de ingresos, costos de reparación de sistemas, o nivel de esfuerzo requerido para corregir el problema causado por la acción exitosa de una amenaza. Otros impactos no pueden ser medidos en términos cuantitativos pero pueden ser calificados o descritos en términos de impacto Alto, Medio y Bajo. En esta investigación se propone una escala general cualitativa, la cual se muestra en la tabla 2.3.

Tabla 2.3. Escala de magnitud de impacto para la valoración del riesgo de TI

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 resultar e 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.

7. *Determinar nivel de riesgo*

- ¿Se han determinado los niveles de riesgo?

El objetivo de este paso es determinar el nivel de riesgo para cada evento identificado (par amenaza / vulnerabilidad), en función del nivel de probabilidad y la magnitud del impacto. En caso de que ambos elementos hayan sido cuantificables, se puede emplear la expresión 2.3 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 organización donde se aplique.

$$NR=NP*MI \qquad (2.3)$$

Donde:

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

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

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 figura 2.5. 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.

Nivel de Probabilidad	Magnitud del impacto		
	Bajo	Medio	Alto
Alto	BAJO	MEDIO	ALTO
Medio	BAJO	MEDIO	MEDIO
Bajo	BAJO	BAJO	BAJO

Figura 2.5. Matriz para determinar nivel de riesgo de TI

Como se puede apreciar en la matriz definida el Nivel de Riesgo se clasifica según la escala siguiente:

-Alto: Existe una fuerte necesidad de establecer medidas correctivas inmediatamente.

-Medio: Se necesitan acciones correctivas, debe desarrollarse un plan para implementarlas en un periodo razonable de tiempo.

-Bajo: Debe determinarse si se necesitan acciones correctivas o se decide aceptar el riesgo.

8. *Recomendar controles*

En este paso deben recomendarse los controles que puedan mitigar o eliminar los riesgos identificados. El objetivo de estos controles es reducir los niveles de riesgo a un valor aceptable. Los controles recomendados son resultado de la valoración del riesgo realizada.

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. Este reporte puede ser útil para apoyar la toma de decisiones del personal de TI y administrativo. Para diseñar este reporte se propone que el registro de la información sea estructurado con el modelo mostrado en la tabla 2.4.

Tabla 2.4. Modelo de reporte de valoración del riesgo de TI

Categoría de Riesgo	N	Vulnerabilidad	Amenaza	Descripción del riesgo	Controles existentes	Nivel de probabilidad	Magnitud del impacto	Nivel de Riesgo	Controles recomendados

Etapa 5: Caracterización del grado de satisfacción de los trabajadores con los recursos y servicios de TI

La inclusión de esta etapa dentro del procedimiento de diagnóstico está dada por la especial importancia que posee el grado de satisfacción de los trabajadores con los recursos y servicios de TI, para los procesos de gestión de TI y por ende para su evaluación. Para la caracterización fue diseñada una encuesta.

Para la aplicación de esta encuesta, en los casos en que no sea posible encuestar el total de trabajadores, se puede realizar un tipo de muestreo estratificado proporcional por área y categoría ocupacional de todos los trabajadores de la organización. La realización de este tipo de muestreo permitirá descubrir si existen diferencias estadísticas significativas entre las opiniones emitidas por personal que pertenece a diferentes categorías ocupacionales y a diferentes áreas.

Etapa 6: Realización del diagnóstico de madurez de los objetivos de control de TI

Para la realización del diagnóstico de madurez se realizan los pasos siguientes:

6.1. *Definir los dominios y objetivos de control a diagnosticar*

En este paso se definen los dominios a diagnosticar y los objetivos de control correspondientes a cada dominio. Se propone partir del modelo COBIT 4.1 (2007) como propuesta general, que debe ser adaptada por el equipo de trabajo considerando elementos (dominios u objetivos de control) a incluir o eliminar en función de las características de la organización donde se aplique.

6.2. *Realizar la recopilación, verificación y análisis de información*

Debe aplicarse la guía de entrevista mostrada en el Anexo 2. La aplicación de los instrumentos diseñados debe estar apoyada por la observación directa y la revisión de documentos.

6.3. ***Determinar el nivel de madurez de cada objetivo de control***

En función de los resultados anteriores, en este paso 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). Esta calificación estará

basada en los modelos de madurez definidos por COBIT, estando definido un modelo para cada objetivo de control.

Etapa 7: Evaluación de la gestión de TI en la organización

En esta etapa se realiza la evaluación de la gestión de TI en la empresa a través del indicador definido en esta investigación, ***Nivel de la Gestión de TI (I_{GTI})***. Los pasos para desarrollar esta etapa son:

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

Para determinar el peso o importancia relativa de cada dominio y de cada objetivo de control se pueden utilizar varios métodos de cálculo subjetivos para la determinación del peso de cada criterio (Triángulo de Füller, Asignación probabilística de Rietveld, AHP de Saaty, Tasación Simple, Comparaciones sucesivas, Asignación directa por ratios).

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:

$$EOC_{dg} = \frac{W_{dg}\, xNM_{dg}}{5} \qquad (2.4)$$

Siendo:

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

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

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:

$$RD_g = \sum_{d=1}^{m_g} EOC_{dg} \qquad (2.5)$$

Siendo:

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:

$$ED_g = W_g \times RD_g \times 100 \qquad (2.6)$$

Siendo:

ED_g : Evaluación del dominio g.

W_g : peso del dominio g.

7.3. *Determinación del indicador I_{GTI}. 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})*** señalado en la expresión 2.7. Su escala se muestra en la tabla 2.5.

$$I_{GTI} = \sum_{g=1}^{4} ED_g \qquad (2.7)$$

Tabla 2.5. Escala para la evaluación de la gestión de TI

Intervalos de I_{GTI} (%)	**Evaluación de la gestión de TI**
($95 \leq I_{GTI} \leq 100$)	Nivel 5: OPTIMIZADO
($75 \leq I_{GTI} < 95$)	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

Para analizar la evaluación obtenida se recomienda representar gráficamente los resultados. Se propone el uso de radares de control para observar el nivel que representa la evaluación del dominio respecto a su evaluación ideal y de manera similar la evaluación de cada objetivo de control dentro de su dominio. La observación de los radares de control le permitirá a la empresa analizar las brechas existentes e incidir en aquellos elementos de peores resultados, tratando de mantener un equilibrio entre todos los dominios. La figura 2.6 muestra ejemplos del empleo de este tipo de gráficos.

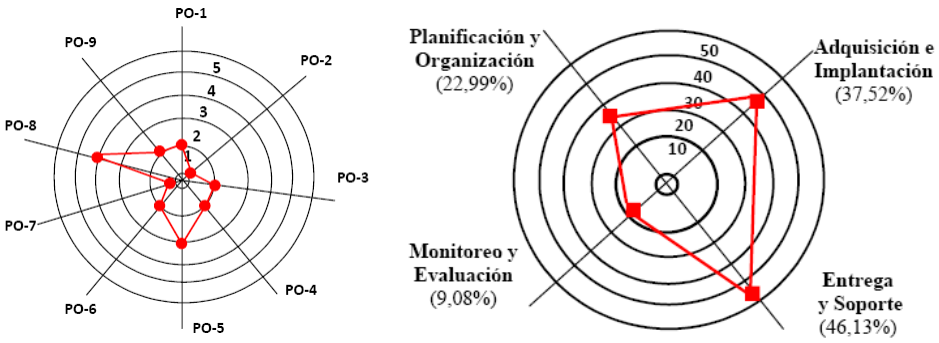


Figura 2.6. Ejemplos de radares de control

Se recomienda además para graficar la influencia de cada dominio y sus objetivos de control, la construcción de un gráfico Causa – Efecto como el representado en la figura 2.7. En el mismo, se reflejarán por dominio los objetivos de control que presentaron dificultades considerando su nivel de madurez; pudiendo llegar a niveles mayores de detalle.

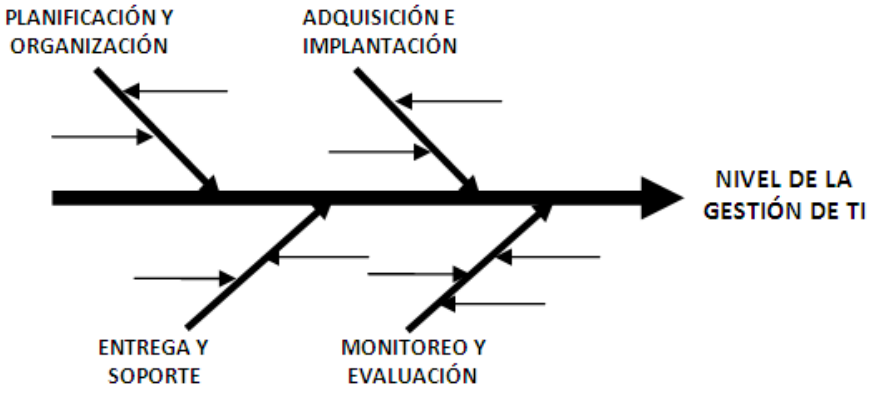


Figura 2.7. Diagrama Causa – Efecto del Nivel de la Gestión de TI

7.4. *Elaboración del informe de evaluación*

A partir de los resultados obtenidos en las etapas precedentes en este paso se deberá elaborar un informe donde se incluya la valoración de: el análisis de los recursos de TI y su alineación a los objetivos de negocio, el análisis de la administración de los riesgos TI, el análisis de la caracterización de la satisfacción de los trabajadores y una relación de los dominios y objetivos de control que reflejaron mayores dificultades en la evaluación de la gestión. Deben señalarse los principales problemas que afectan la gestión de TI en la organización.

En este momento se cuenta con una evaluación del estado actual de la gestión de TI en la organización y el análisis de los principales problemas que inciden en los resultados obtenidos, finalizando la primera fase del estudio. En función de corregir o mejorar los problemas analizados, se plantea la etapa 8 que constituye una interface que sienta las bases para iniciar la fase correspondiente al diseño del proceso de gestión de TI en la organización objeto de estudio.

Etapa 8: Propuesta de medidas correctivas, preventivas y/o de mejora

Una vez realizada 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 esta etapa se procede a elaborar la propuesta de dichas acciones.

2.2. Caracterización de las empresas objeto de estudio

2.2.1. UEB de Ingeniería y Servicios Técnicos Azucareros (TECNOAZUCAR VC)

TECNOAZUCAR es una empresa cubana, fundada en 1982, por el Ministerio del Azúcar de Cuba, especializada en la exportación al exterior y venta en el mercado interno de azúcares y sus productos derivados, así como la prestación de servicios técnicos, consultoría, asistencia técnica y transferencia de tecnologías hacia diversos países del mundo.

En conformidad con las leyes cubanas, TECNOAZUCAR es una empresa autofinanciada, con personalidad jurídica, administración y capital propios, lo cual permite actuar con independencia en la comercialización de los servicios y productos que oferta.

Sus ofertas están respaldadas por la experiencia y la fuerza técnica de la industria azucarera cubana, organizada en 71 fábricas de azúcar, 14 centrales mieleras, 14 destilerías y fábricas de ron, 12 fábricas de levadura torula y mieles deshidratadas, 4 fábricas de tableros de bagazo y otras instalaciones que producen diversos derivados de la caña.

La UEB de Ingeniería y Servicios Técnicos Azucareros (TECNOAZUCAR VC) fue creada según la Resolución No 89 5/11/2010 la misma tiene domicilio en calle Alemán No 57 entre Rafael Tristá y Padre Chao, Santa Clara.

Su **misión** es producir y comercializar productos y servicios de excelencia generados por el desarrollo y la diversificación de la Agroindustria azucarera, logrando la plena satisfacción de nuestros clientes conscientes de nuestra responsabilidad social y medioambiental. Tiene como **visión** ser una empresa perfeccionada de 1er nivel, con un Sistema de Gestión de la Calidad Acreditado según las normas internacionales exigidas para nuestra actividad, que nos permita satisfacer las necesidades de nuestros clientes brindándoles servicios y productos de excelencia.

Principales Clientes: Los portales S.A, Cubaron (Ronera Central), todos los hoteles de la Cayería (Gaviota), Cadena de Tiendas CIMEX, Complejo de tiendas TRD, MINAL (Cervecería, Confitería, Lácteos), CORACAN, CORALAC, PAPAS & Co, SUCHEL

Productos que comercializa:

- Mieles (miel final, miel B, otras mieles)
- Alcoholes (alcoholes finos, alcohol técnico ¨A¨, alcohol técnico B¨, alcohol desnaturalizado F5, gel de alcoholes, otros derivados del Alcohol)
- Caramelos (caramelos envueltos, caramelos desnudos, siropes saborisados, siropes para coctelería, tableros y derivados del bagazo, tableros de fibras, tableros de partículas, otros derivados del bagazo, sorbitol, azúcar crudo granel, vinagre, productos gydema, gas carbónico, ceras fural)
- Productos cárnicos (productos del ganado vacuno, embutidos y otros derivados del cerdo, otros productos cárnicos, conservas)
- Azúcares (azúcar crudo a granel, azúcar crudo ensacado, azúcar refino ¨A¨, azúcar ¨Buen Día¨, azúcar ecológica, minidosis de azúcar, otros azúcares)
- Bebidas alcohólicas (Ron refino, Ron Silver Dry, Ron Carta Blancal, Ron Palma, Ron Solera, Ron Añejo Ambarino, Ron Añejo Reserva, Ron Añejo Oscuro, Aguardientes, Vodka, Licores y Cremas, Elixir de Ron, Minidosis de Rones y Aguardientes)

2.2.2. Empresa de Tecnología de la Información y Automática (ATI)

Perteneciente al ministerio de la industria básica y con domicilio en la calle Campo esq. Central, Santa Clara, Villa Clara, la Empresa de Tecnología de la Información y Automática es una entidad prestadora de servicios que tiene como **misión:** prestar servicios integrales de ingeniería y proyectos en la rama de competitividad al Sistema Electroenergético Nacional y a otros clientes.

Su **visión**: ser un centro de servicios técnicos especializados de alto prestigio en la rama de la Instrumentación y la Automatización Industrial, que inspire seguridad y confianza a sus clientes, y que sea líder en la aplicación de la ciencia y la técnica en su trabajo.

Principales clientes: Central termoeléctrica Antonio Guiteras, Central termoeléctrica Carlos M. de Céspedes, Hidroeléctrica Hanabanilla, Hidroeléctrica Zaza, Empresas eléctricas provinciales y municipales, Grupos electrógenos y otras entidades de la industria básica.

Servicios que presta:

- Mantenimiento y reparación de equipos de medición eléctricos, electrónicos, neumáticos, patrones eléctricos y digitales
- Control metrológico
- Diseño y montaje de sistemas de protecciones eléctricas
- Servicios de ingeniería de automatización industrial

La UEB ATI Villa Clara, perteneciente a la Empresa de Tecnología de la Información y Automática, se ha trazado como política:

- Prestar servicios técnicos de alta calidad, orientando su trabajo hacia el logro de la plena satisfacción de los clientes y el mejoramiento continuo de los procesos internos.
- Trabajar por la preservación del medio ambiente y la disminución de los riesgos para la seguridad y salud de los trabajadores.

Para este propósito se ha implementado un Sistema de Gestión de la Calidad basado en la NC ISO 9001:2008 y se trabaja en la integración progresiva con los sistemas de gestión de medio ambiente y el de seguridad y salud en el trabajo, basados en las NC ISO 14001: 2004 y la NC 18001:2005 respectivamente.

Su **cartera de servicios** incluye:

- Servicios técnicos integrales en la especialidad de Automatización Industrial.

1. Diseño de ingeniería básica e ingeniería de detalle.

2. Ejecución de los proyectos.

3. Servicios de postventa

4. Servicios integrales de asistencia técnica.

- Proyectos "llave en mano" para la automática y la electricidad de nuevas instalaciones o modernización de las existentes, que pueden incluir desde los estudios de factibilidad, la ingeniería básica, la ingeniería de detalle, la gestión de suministros, la ejecución de los proyectos y la puesta en marcha.
- Servicios integrales de metrología, que abarca la calibración y las soluciones técnicas necesarias a instrumentos de medición, sensores y lazos de medición de parámetros tecnológicos de los sistemas industriales de Instrumentación y Control (I&C).
- Servicios de verificación de metros contadores industriales de energía eléctrica
- Ejecución de auditorías y consultarías en las especialidades de calidad, automática y metrología a las entidades de la UNE.
- Participación en los procesos inversionistas de la UNE que realice nuestra Empresa Nacional (estudios de factibilidad, contratación, ejecución y puesta en marcha).
- Diseño y fabricación "a pedido" de equipos, instrumentos, accesorios o partes para Sistemas de Instrumentación y Control (I&C).
- Soluciones técnicas para garantizar la explotación y el mantenimiento de equipos especiales y sistemas de medición y/o control de alta complejidad en la especialidad de automática de las centrales eléctricas.
- Proyectos para suministro eléctrico de instalaciones industriales, hoteles y otros.
- Proyectos de aterramiento y protección contra sobre voltaje de instalaciones industriales, hoteles y otros.

Esta empresa trabaja dentro del sector de la Ingeniería, el cual consideran en fase emergente en la actualidad, después de haber sufrido una descapitalización provocada por la brusca interrupción de inversiones en el país. Las tendencias de desarrollo de este sector son evidentes, ya que el renacimiento del proceso inversionista y la aplicación consecuente de las indicaciones de la resolución económica del V Congreso del PCC aseguran un incremento en la demanda de servicios especializados de Ingeniería. Esta explosión de necesidades de nuevos proyectos y servicios técnicos ofrece a ATI amplias posibilidades de

nuevos trabajos, pero también la somete a una amenaza permanente con la aparición de nuevas organizaciones dedicadas a la ingeniería y el diseño, quienes constituyen competidores fuertes dentro de este mercado de trabajo.

2.3. Conclusiones parciales

Una vez concluido el desarrollo de este capítulo se llegaron a las siguientes conclusiones parciales**:**

1. El procedimiento general para el diagnóstico de la gestión de TI, permite analizar la alineación entre procesos de negocio y recursos de TI, analizar la administración de los riesgos y evaluar el nivel actual de gestión en función de la mejora continua en la organización; llevando a cabo los procesos complejos que esto incluye, de forma relativamente sencilla, el mismo puede ser aplicado por la propia organización como herramienta de autoevaluación, monitoreo y mejora, eliminando las limitantes y dificultades de aplicar auditorías externas con fines similares.
2. El procedimiento general permite la integración del modelo COBIT con herramientas de evaluación de alineación de recursos de TI, considerando la satisfacción de los trabajadores; lo que permite un diagnóstico integral de la gestión de TI en la organización.
3. El indicador integral (I_{GTI}) para la evaluación de la gestión de TI basado en el modelo COBIT y la evaluación de madurez de procesos permite medir el nivel de la gestión de TI en una organización, expresando una medida única e integral.

Capítulo 3. Aplicación del procedimiento en las empresas

Este capítulo tiene como objetivo principal la aplicación de las etapas y pasos del procedimiento para diagnosticar el estado actual de la gestión de TI, en las empresas TECNOAZUCAR y ATI de la provincia de Villa Clara. A partir del estudio se identificaron los principales problemas que presentan y las oportunidades de mejora de la gestión de TI que contribuyen a comprender y evaluar los riesgos y beneficios asociados con estos recursos en ambas organizaciones.

3.1. Aplicación del procedimiento en las empresas objeto de estudio

El procedimiento general descrito en el Capítulo 2 fue aplicado en las empresas TECNOAZUCAR y ATI Los resultados obtenidos a través de las distintas etapas se muestran simultáneamente para ambas empresas.

3.1.1. Desarrollo de las etapas 1 y 2

En esta etapa quedó definida la estructura del equipo de trabajo de cada empresa y la cantidad de miembros de cada uno y fue seleccionado el personal, asignándose las responsabilidades y las tareas a realizar. Además se conformó el grupo de expertos de ambas empresas como se muestra en el cuadro 3.1.

Cuadro 3.1. Personal que integra el grupo de expertos en ambas empresas

Cargo o especialidad	Nombre y apellidos	Cargo o especialidad	Nombre y apellidos
	TECNOAZUCAR		ATI
Director	Mario E. García Muñoz	Director	Gustavo Choy Pérez
Calidad	Dulce M. Pérez	Calidad	Emérita Veitía Álvarez
Comercial	Livan Pérez Rodríguez	Administrador de red	Glenda Moreno
Informática	Danny Jiménez Sabina	Informática	Elismary Roque
Jefe Económico	Ania Ortís Campo	Jefe Económico	Osmelvy Bermúdez
Jefe de Recursos Humanos	Leonardo Fernández Alberto	Jefe de Recursos Humanos	Saraí Arbelo Ruiz

Las caracterizaciones de ambas organizaciones se muestran en el Capítulo 2.

3.1.2. Etapa 3: Análisis de los recursos de TI y su alineación a los objetivos de negocio de la organización

3.1. *Inventario de los recursos de TI de la organización*

Las empresas TECNOAZUCAR y ATI cuentan con un especialista y un jefe de seguridad informática siendo ambos los encargados de la actividad de TI en cada una. Poseen un total de 25 computadoras, 3 servidores y 50 computadoras, 4 servidores respectivamente que soportan todas las actividades, así como la red interna y demás servicios. Por parte de TECNOAZUCAR los principales sistemas de gestión son el VERSAT, RH EXPERT y el ENERGEST y en el caso de ATI son el ASSET PREMIUM, CFT y GTP los cuales automatizan todas las actividades de las entidades.

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 las organizaciones se procedió a efectuar una clasificación de los mismos en función de su impacto en el negocio, que se apoyó en el algoritmo de la figura 2.2 del capítulo anterior y de la realización de entrevistas al personal. En el Anexo 3 a) y b) se muestra el inventario realizado en ambas empresas.

Utilizando las expresiones propuestas (2.1 y 2.2) fue clasificado el impacto global y de cada tipo de recurso. Los resultados de los mismos se muestran en la tabla 3.1.

Tabla 3.1. Clasificación de los recursos de TI

Índice relativo	**Resultado de los índices según clasificación j**			
	TECNOAZUCAR	**Clasificación**	**ATI**	**Clasificación**
Global ($IRTI_j$)	Débil = 6.67% Medio =16.67% Fuerte =73.33%	Fuerte	Débil =1.75% Medio=56.14% Fuerte=57.89%	Fuerte
IRR_{ij} i : Personal	Medio =100%	Medio	Medio =100%	Medio
IRR_{ij} i : Aplicaciones	Medio =33.33% Fuerte =66.67%	Fuerte	Fuerte =100 %	Fuerte
IRR_{ij} i : Infraestructura	Débil = 8% Medio =16% Fuerte = 76 %	Fuerte	Débil = 1.92 % Medio=61.54% Fuerte=36.54%	Medio

Puede apreciarse que el impacto global en ambas fue calificado de Fuerte, al ser clasificados así 73.33% y el 57.89% del total de recursos respectivamente. El recurso que tiene mayor cantidad de impactos fuertes en el caso de TECNOAZUCAR es el de

infraestructura pues estos representan el 76% del total, siendo en ATI el de aplicaciones con el 100%.

3.3. *Evaluación de los procesos de negocio en función de su grado de dependencia de TI*

En ambas empresas se puede afirmar que los procesos de negocio poseen una dependencia fuerte de las tecnologías de la información, pues son un elemento fundamental en la estrategia de negocio de las organizaciones, debido a que determinan totalmente la ejecución de los procesos de negocio. Son indispensables para obtener los servicios brindados.

3.4. *Análisis de la correspondencia entre los recursos de TI y los requerimientos de la organización en función de sus objetivos de negocio*

Después de analizar la correspondencia existente entre los recursos de TI y los requerimientos de las organizaciones se observó que presentan una alineación adecuada para satisfacer los requerimientos de ambas, pues los recursos de TI poseen un impacto fuerte en las dos, mientras que los procesos de negocio poseen una dependencia Fuerte de las tecnologías de la información.

3.1.3. Etapa 4: Análisis de los riesgos de TI y su administración

En las empresas se realiza la evaluación de riesgos como parte fundamental de la actividad de seguridad informática, ésta se apoya además del Plan de Seguridad Informática en el cual queda plasmado todo el resultado de dicho análisis, así como las políticas a seguir para evitar que ocurran o mitigar dichos riesgos. Tienen identificados los recursos críticos de TI, sin embargo en TECNOAZUCAR no se tienen declaradas todas las vulnerabilidades y las amenazas que pueden ser origen a los riesgos identificados o provocar otros. Tienen identificado además el nivel de riesgo, pero no así la categoría correspondiente, este análisis se pudo realizar en TECNOAZUCAR pero en ATI no, debido que ellos consideran que esta información debe ser parte de la confidencialidad de la empresa. Poseen controles técnicos como mecanismos de identificación, y controles de accesos y controles no técnicos como políticas de seguridad, medidas de seguridad de personal, etc. La documentación de los resultados obtenidos en esta etapa para la empresa TECNOAZUCAR se muestran en el modelo de reporte de valoración del riesgo de TI en el Anexo 4.

3.1.4. Etapa 5: Caracterización del grado de satisfacción de los trabajadores con los recursos y servicios de TI

En esta etapa se aplicó la encuesta para caracterizar el grado de satisfacción de los trabajadores. Siendo la plantilla total de 92 trabajadores en ATI y 75 en TECNOAZUCAR, de los cuales 42 y 34 no interactúan nunca con los recursos de TI, se decidió muestrear a todo el personal restante.

En TECNOAZUCAR el 76% de los encuestados se encuentra satisfecho con la calidad de la infraestructura de TI que utilizan, y el 24% se encuentra medianamente satisfecho. La satisfacción respecto a la disponibilidad de la infraestructura es del 40% siendo la más baja, quedando el 60% medianamente satisfecho. Con relación a la correspondencia entre las características de la infraestructura de TI, a la correspondencia entre las funcionalidades que brindan los software y la correspondencia entre los servicios que se ofrecen y las necesidades de trabajo el 72% está satisfecho en relación a las dos primeras y el 76 % con la última, quedando el resto de cada una medianamente satisfecho. Cabe destacar que respecto a la calidad de los mantenimientos y su frecuencia están satisfechos solo el 68% y 60% respectivamente, lo que no está del todo mal pero se debiera aspirar alcanzar una mejor porciento. La satisfacción respecto a la atención que brinda el personal de TI es del 76%, el resto se encuentra medianamente satisfecho. El interés de la dirección de la empresa con respecto a la capacitación es del 64% de satisfacción. Todas las preguntas de esta encuesta fueron valoradas entre satisfecho y medianamente satisfecho La satisfacción general con los recursos y servicios de TI fue calificada de media en el 68% de los casos.

Sin embargo en ATI el 58% esta satisfecho y el 42% medianamente satisfecho en relación con la calidad de la infraestructura que utilizan. En relación a la disponibilidad de la infraestructura el 54% se encuentra satisfecho y el 46% medianamente satisfecho. La calidad del servicio de Internet es del 38% de satisfacción de los encuestados siendo la más baja de todas. La correspondencia entre las características de la infraestructura de TI, la correspondencia entre las funcionalidades que brindan los software y la correspondencia entre los servicios que se ofrecen y las necesidades de trabajo el 52%, 66% y 58% se encuentra satisfecho, respectivamente. La calidad de los mantenimientos, así como las frecuencias tienen el 66% y 64% de satisfacción respectivamente, pudiendo aspirarse a

mejor porciento. Respecto a la atención que brinda el personal de TI el 66% está satisfecho. D e manera general la satisfacción con los recursos de y servicios de ti es media siendo 55.1% de los casos.

Fue evaluada la fiabilidad del cuestionario para la totalidad de los ítems, obteniéndose un Alfa de Cronbach de 0.879 en ATI y para 0.778 TECNOAZUCAR de un criterio bastante extendido para interpretar este coeficiente es que ha de ser igual o superior a 0.70 (Nunnally, 1978), por lo puede afirmarse que el cuestionario tiene una fiabilidad suficiente

3.1.5. Etapa 6: Realización del diagnóstico de madurez de los objetivos de control

6.1. *Definir los dominios y objetivos de control a diagnosticar*

Los dominios y objetivos de control a diagnosticar que fueron definidos en ambas empresas en función de sus características se muestran en el cuadro 3.2. Seguidamente se muestra un resumen de la información obtenida por cada objetivo de control.

3.1.5.1. Caso de estudio TECNOAZUCAR

Planificación y Organización

Definir plan estratégico para TI: Existe en la empresa un plan estratégico de TI, está establecido cómo y cuándo realizar dicha planeación la cual se discute y controla en las reuniones del negocio, máximo 2 veces al año. Incluye una definición clara de los riesgos que la empresa puede afrontar respecto a estos recursos.

Definir la arquitectura de información: La arquitectura de la información en la entidad se entiende y acepta, y la responsabilidad de su aplicación se asigna y se comunica de forma clara. Se han desarrollado políticas básicas de arquitectura de información, existe una función de administración de datos definida formalmente que establece estándares para toda la organización. Se definen, documentan y aplican actividades de entrenamiento de manera formal.

Cuadro 3.2. Dominios y objetivos de control a diagnosticar

TECNOAZUCAR	*ATI*
Planeación y Organización	
Definir un plan estratégico de TI Definir la arquitectura de la información Determinar la dirección tecnológica Definir los procesos, organización y relaciones de TI Comunicar las aspiraciones y la dirección de la gerencia Administrar los recursos humanos de TI Administrar la calidad Evaluar y administrar los riesgos de TI	Definir un plan estratégico de TI Definir la arquitectura de la información Determinar la dirección tecnológica Definir los procesos, organización y relaciones de TI Comunicar las aspiraciones y la dirección de la gerencia Administrar la inversión de TI Administrar la calidad Evaluar y administrar los riesgos de TI Administrar proyectos
Adquisición e Implantación	
Identificar soluciones automatizadas Adquirir y mantener infraestructura tecnológica Facilitar la operación y el uso Adquirir recursos de TI. Administrar cambios Instalar y acreditar soluciones y cambios	Identificar soluciones automatizadas Adquirir y mantener software aplicativo Adquirir y mantener infraestructura tecnológica Facilitar la operación y el uso Adquirir recursos de TI Administrar cambios Instalar y acreditar soluciones y cambios
Entrega y Soporte	
Administrar el desempeño y la capacidad Garantizar la continuidad del servicio Garantizar la seguridad de los sistemas Educar y entrenar a los usuarios Administrar la mesa de servicio y los incidentes Administrar los problemas Administrar los datos Administrar el ambiente físico Administrar las operaciones	Definir y administrar los niveles de servicio Administrar los servicios de terceros Administrar el desempeño y la capacidad Garantizar la continuidad del servicio Garantizar la seguridad de los sistemas Educar y entrenar a los usuarios Administrar la mesa de servicio y los incidentes Administrar la configuración Administrar los datos
Monitoreo y Evaluación	
Monitorear y evaluar el desempeño de TI Monitorear y evaluar el control interno Garantizar el cumplimiento regulatorio Proporcionar gobierno de TI	Monitorear y evaluar el desempeño de TI Monitorear y evaluar el control interno Garantizar el cumplimiento regulatorio Proporcionar gobierno de TI

Determinar la dirección tecnológica: Aunque no cuentan con un plan de infraestructura tecnológica, la dirección reconoce la necesidad de poseer uno. La dirección tecnológica está impulsada por los planes evolutivos del hardware, software de sistema y de los proveedores de software aplicativo.

Definir los procesos, organización y relaciones de TI: Existen roles y responsabilidades definidas para la organización de TI. La organización se desarrolla, documenta, comunica y se alinea con la estrategia de TI. Se define el ambiente de control interno y las auditorías internas. Existen definiciones de las funciones a ser realizadas por parte del personal de TI y las que deben realizar los usuarios. La división de roles y responsabilidades está definida e implementada.

Comunicar las aspiraciones y la dirección de la gerencia: El proceso de elaboración de políticas es estructurado, mantenido y conocido por el personal, y las políticas, procedimientos y estándares existentes son razonablemente sólidos y cubren temas clave. La gerencia ha reconocido la importancia de la conciencia de la seguridad de TI y ha iniciado programas de concienciación. Aunque existe un marco general de desarrollo para las políticas y estándares de control, el monitoreo del cumplimiento de estas políticas y estándares es inconsistente. Las técnicas para fomentar la conciencia de la seguridad están estandarizadas y formalizadas.

Administrar los recursos humanos de TI: El proceso de recursos humanos está enfocado de manera operacional en la contratación y administración del personal de TI. Se está desarrollando la conciencia con respecto al impacto que tienen los cambios rápidos de negocio, de tecnología y las soluciones cada vez más complejas, sobre la necesidad de nuevos niveles de habilidades y de competencia.

Administrar la calidad: Existe conciencia por parte de la dirección de la necesidad de un sistema de gestión de calidad. El sistema de gestión de calidad es impulsado por individuos cuando este ocurre. La dirección realiza juicios informales sobre la calidad.

Evaluar y administrar los riesgos de TI: Existe un enfoque de evaluación de riesgos inmaduro y en evolución. La administración de riesgos se da por lo general a altos niveles y se aplica de manera típica solo como respuesta a problemas. Los procesos de mitigación de riesgos están en implementación donde se identifican riesgos.

Adquisición e Implementación

Identificar soluciones automatizadas: Existen algunos enfoques intuitivos para identificar que existen soluciones de TI y que estas varían a lo largo del negocio. Las soluciones se identifican de manera informal con base en la experiencia interna y en el conocimiento de la función de TI. Se usan enfoques no estructurados para definir los requerimientos e identificar las soluciones tecnológicas.

Adquirir y mantener software aplicativo: La empresa cuenta con un claro, definido y generalmente entendido proceso para dar mantenimiento a la infraestructura de TI. El proceso respalda las necesidades de las aplicaciones críticas del negocio y concuerda con la estrategia de negocio de TI. El mantenimiento se planea, programa y coordina.

Facilitar la operación y el uso: Se cuenta con un esquema bien definido, aceptado y comprendido para la documentación del usuario, manuales de operación y materiales de entrenamiento. Las correcciones a la documentación y a los procedimientos se realizan por reacción. Los procedimientos se encuentran disponibles fuera de línea y se pueden acceder y mantener en caso de desastres. Existe un proceso que especifica las actualizaciones de los materiales de entrenamientos. Se planea y programa tanto el entrenamiento del negocio como de los usuarios.

Adquirir recursos de TI: La organización ha reconocido la necesidad de tener políticas y procedimientos documentados que enlacen la adquisición de TI con el proceso general de adquisiciones de la organización. Los contratos para la adquisición de recursos de TI son elaborados y administrados por gerentes de proyecto y otras personas que ejercen su juicio profesional más que seguir resultados de procedimientos y políticas formales.

Administrar cambios: El proceso de administración de cambio se desarrolla bien y es consistente para todos los cambios. El proceso se basa en manuales de procedimientos y controles. La documentación de administración de cambios de TI está vigente y correcta. La planeación e implantación de la administración de cambios de TI se van integrando con los cambios en los procesos de negocio para asegurar que se resuelven los asuntos referentes al entrenamiento, cambio organizacional y continuidad del negocio.

Instalar y acreditar soluciones y cambios: Existe cierta consistencia entre los enfoques de prueba y acreditación pero no se basan en ninguna metodología. Los equipos individuales

de desarrollo deciden normalmente el enfoque de prueba y casi siempre hay ausencia de pruebas de integración. Hay un proceso de aprobación informal.

Entrega y Soporte

Administrar los servicios de terceros: El proceso de supervisión de los proveedores de servicios de terceros, de los riesgos asociados y de la prestación de servicios es informal. Se utiliza un contrato pro-forma con términos y condiciones estándares del proveedor (por ejemplo, la descripción de servicios que se prestarán). Los reportes sobre los servicios existen, pero no apoyan los objetivos del negocio.

Administrar el desempeño y la capacidad: Las necesidades de desempeño se logran por lo general con base en evaluaciones de sistemas individuales y el conocimiento y el soporte de equipos de proyectos. Algunas herramientas individuales pueden utilizarse para diagnosticar problemas de desempeño y de capacidad. No hay evaluación general de la capacidad de desempeño de TI. Cualquier medición de desempeño se basa en las necesidades de TI.

Garantizar la continuidad del servicio: Las responsabilidades de la planeación y de las pruebas de continuidad de los usuarios están claramente asignadas y definidas. El plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto del negocio. La gerencia comunica la necesidad de planear el aseguramiento de la continuidad del servicio.

Garantizar la seguridad de los sistemas: Existe conciencia sobre la seguridad y es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, además de contar con un plan de seguridad de TI y algunas soluciones motivadas por un análisis de riesgo. Existe capacitación con respecto a seguridad de TI la cual se programa y comunica de manera formal.

Educar y entrenar a los usuarios: El programa de entrenamiento y educación se institucionaliza y comunica, los empleados y gerentes identifican las necesidades de entrenamiento. Para soportar el programa de entrenamiento y educación se establecen presupuestos, recursos, instructores e instalación, se imparten clases formales sobre conducta ética, conciencia y prácticas de seguridad.

Administrar la mesa de servicio y los incidentes: Se reconoce y se acepta la necesidad de contar con una función de mesa de servicio y un proceso para la administración de incidentes. Las consultas y los incidentes se rastrean de forma manual y se monitorean de forma individual, pero no existe un sistema formal de reporte. No se mide la respuesta oportuna a las consultas e incidentes y los incidentes pueden quedar sin resolución. Los usuarios han recibido indicaciones claras de dónde y cómo reportar problemas e incidentes.

Administración de problemas: Se estandarizan los procesos de escalamiento y resolución de problemas. El registro y rastreo de problemas y de sus soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles sin centralizar. La información se comparte entre el personal de manera formal y proactiva. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.

Administración de datos: Se entiende y se acepta la necesidad de la administración de datos, tanto dentro de TI como a lo largo de toda la organización. Se establece la responsabilidad sobre la administración de los datos y se asigna la propiedad sobre los datos a la parte responsable que controla la integridad y la seguridad. Los procedimientos de administración de datos se formalizan dentro de TI y se utilizan herramientas para respaldar la recuperación y desecho. Se imparten entrenamientos acerca de la administración de datos.

Administración del ambiente físico: Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlados. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado. Se aplican restricciones de acceso permitiendo el ingreso a las instalaciones de cómputo solo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo.

Administración de operaciones: Se entiende y se acepta dentro de la organización la necesidad de administrar las operaciones de cómputo. Se han asignado recursos y se lleva a cabo alguna capacitación. Las funciones repetitivas están definidas, estandarizadas, documentadas y comunicadas de manera formal. Se desarrolla una política formal para reducir el número de eventos no programados. Los resultados de las tareas completadas y de los eventos se registran con reportes limitados hacia la gerencia.

Monitoreo y Evaluación

Monitorear y evaluar el desempeño de TI: Se han implantado programas educacionales y de entrenamiento para el monitoreo. Se ha desarrollado una base de conocimiento formalizada del desempeño histórico y se ha definido un guía para medir el desempeño.

Monitorear y evaluar el control interno: La dirección apoya el monitoreo del control interno. Se han desarrollado políticas y procedimientos para evaluar y reportar las actividades de monitoreo del control interno. Las políticas de evaluación de riesgos de los procesos de TI se utilizan dentro de los marcos de trabajo desarrollados de manera específica para la función de TI.

Garantizar el cumplimiento regulatorio: Existe un esquema formal de entrenamiento que asegura que todo el personal esté consciente de sus obligaciones de cumplimiento. Existe un mecanismo implantado para monitorear el no cumplimiento de los requisitos internos, reforzar las prácticas internas e implantar acciones correctivas. Los eventos de no cumplimiento se analizan de forma estándar en busca de las causas.

Proporcionar gobierno de TI: Existe una conciencia sobre los temas de gobierno de TI. Las actividades y los indicadores de desempeño del gobierno de TI están en desarrollo. Los procesos, herramientas y métricas para medir el gobierno de TI son limitados y pueden no usarse a toda su capacidad debido a la falta de experiencia en su funcionalidad.

3.1.5.2. Caso de estudio ATI

Planificación y Organización

Definir un plan estratégico de TI: La planeación estratégica de TI sigue un enfoque estructurado, el cual se documenta y se da a conocer a todo el equipo. El proceso de planeación de TI es razonablemente sólido y garantiza que es factible realizar una planeación adecuada. Las estrategias de recursos humanos, técnicos y financieros de TI influencian cada vez más la adquisición de nuevos productos y tecnologías. La planeación estratégica de TI se discute en reuniones de la dirección del negocio.

Definir la arquitectura de la información: Surge un proceso de arquitectura de información y existen procedimientos similares, aunque intuitivos e informales, que se siguen por distintos individuos dentro de la organización. Las personas obtienen sus habilidades al

construir la arquitectura de información por medio de experiencia práctica y la aplicación repetida de técnicas.

Determinar la dirección tecnológica: Se difunde la necesidad e importancia de la planeación tecnológica. La planeación es táctica y se enfoca en generar soluciones técnicas a problemas técnicos. Las personas obtienen sus habilidades sobre planeación tecnológica a través de un aprendizaje práctico y de una aplicación repetida de las técnicas. Están surgiendo técnicas y estándares comunes para el desarrollo de componentes de la infraestructura.

Definir los procesos, organización y relaciones de TI: La organización de TI se desarrolla, documenta, comunica y se alinea con la estrategia de TI. Existen definiciones de las funciones a ser realizadas por parte del personal de TI y las que deben realizar los usuarios. Los requerimientos esenciales de personal de TI y experiencia están definidos y satisfechos. La división de roles y responsabilidades está definida e implantada.

Administrar la inversión en TI: Existe un entendimiento implícito de la necesidad de seleccionar y presupuestar las inversiones en TI. La necesidad de un proceso de selección y presupuesto se comunica. Surgen técnicas comunes para desarrollar componentes del presupuesto de TI. Se toman decisiones presupuestales reactivas y tácticas.

Comunicar las aspiraciones y la dirección de la gerencia: La gerencia ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información, que incluye un marco para las políticas, procedimientos y estándares. La gerencia ha reconocido la importancia de la conciencia de la seguridad de TI y ha iniciado programas de concienciación.. Las técnicas para fomentar la conciencia de la seguridad están estandarizadas y formalizadas.

Administrar la calidad: El QMS está incluido en todos los procesos, incluyendo aquellos que dependen de terceros. Se está estableciendo una base de conocimiento estandarizada para las métricas de calidad. Se ha institucionalizado un programa de educación y entrenamiento para educar a todos los niveles de la organización en el tema de la calidad. Se conducen encuestas de satisfacción de calidad de manera consistente.

Evaluar y administrar los riesgos de TI: La administración de riesgos sigue un proceso definido, el cual está documentado. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se deja a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves para el negocio sean identificados.

Administrar proyectos: La alta dirección ha obtenido y comunicado la conciencia de la necesidad de la administración de los proyectos de TI. La organización está en proceso de desarrollar y utilizar algunas técnicas y métodos proyecto por proyecto. Los proyectos de TI han definido objetivos técnicos y de negocio de manera informal.

Adquisición e Implantación

Identificar soluciones automatizadas: Existen enfoques claros y estructurados para determinar las soluciones de TI. El enfoque para la determinación de las soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del negocio o del usuario, las oportunidades tecnológicas, la factibilidad económica, las evaluaciones de riesgo y otros factores.

Adquirir y mantener software aplicativo: Existe un claro, definido y generalmente entendido proceso para adquirir y dar mantenimiento a la infraestructura TI. El proceso respalda las necesidades de las aplicaciones críticas del negocio y concuerda con la estrategia de negocio de TI, pero no se aplica en forma consistente. Se planea, programa y coordina el mantenimiento. Existen ambientes separados para prueba y producción.

Adquirir y mantener infraestructura tecnológica: Existe un claro, definido y generalmente entendido proceso para adquirir y dar mantenimiento a la infraestructura TI. El proceso respalda las necesidades de las aplicaciones críticas del negocio y concuerda con la estrategia de negocio de TI, pero no se aplica en forma consistente. Se planea, programa y coordina el mantenimiento.

Facilitar la operación y el uso: Existe un esquema bien definido, aceptado y comprendido para documentación del usuario, manuales de operación y materiales de entrenamiento. Los procedimientos se encuentran disponibles fuera de línea y se pueden acceder y mantener en caso de desastre. Se planea y programa tanto el entrenamiento del negocio como de los usuario.

Adquirir recursos de TI: La administración establece políticas y procedimientos para la adquisición de TI. Las políticas y procedimientos toman como guía el proceso general de adquisición de la organización. La adquisición de TI se integra en gran parte con los sistemas generales de adquisición del negocio.

Administrar cambios: Existe un proceso formal definido para la administración del cambio, que incluye la categorización, asignación de prioridades, procedimientos de emergencia, autorización del cambio y administración de liberación, y va surgiendo el cumplimiento. Se dan soluciones temporales a los problemas y los procesos a menudo se omiten o se hacen a un lado.

Instalar y acreditar soluciones y cambios: Existe cierta consistencia entre los enfoques de prueba y acreditación, pero por lo regular no se basan en ninguna metodología. Los equipos individuales de desarrollo deciden normalmente el enfoque de prueba y casi siempre hay ausencia de pruebas de integración. Hay un proceso de aprobación informal.

Entrega y Soporte

Definir y administrar los niveles de servicios: El proceso de desarrollo del acuerdo de niveles de servicio está en orden y cuenta con puntos de control para revalorar los niveles de servicio y la satisfacción de cliente. Los servicios y los niveles de servicio están definidos, documentados y se ha acordado utilizar un proceso estándar. Los niveles de servicio están acordados pero pueden no responder a las necesidades del negocio.

Administrar los servicios de terceros: Hay procedimientos bien documentados para controlar los servicios de terceros con procesos claros para tratar y negociar con los proveedores. Cuando se hace un acuerdo de prestación de servicios, la relación con el tercero es meramente contractual. La naturaleza de los servicios a prestar se detalla en el contrato e incluye requerimientos legales, operativos y de control.

Administrar el desempeño y la capacidad: Los requerimientos de desempeño y capacidad están definidos a lo largo del ciclo de vida del sistema. Los pronósticos de la capacidad y el desempeño se modelan por medio de un proceso definido. Los reportes se generan con estadísticas de desempeño. Los problemas relacionados al desempeño y a la capacidad siguen siendo susceptibles a ocurrir y su resolución sigue consumiendo tiempo.

Garantizar la continuidad del servicio: Se hacen cumplir las responsabilidades y los estándares para la continuidad de los servicios. Se asigna la responsabilidad de mantener un plan de continuidad de servicios. Se recopila, analiza y reporta documentación estructurada sobre la continuidad en los servicios y se actúa en consecuencia

Garantizar la seguridad de los sistemas: Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada.

Educar y entrenar a los usuarios: El programa de entrenamiento y educación se institucionaliza y comunica, y los empleados y gerentes identifican y documentan las necesidades de entrenamiento. Los procesos de entrenamiento y educación se estandarizan y documentan. Para soportar el programa de entrenamiento y educación, se establecen presupuestos, recursos, instructores e instalaciones

Administrar la mesa de servicio y los incidentes: La gerencia reconoce que requiere un proceso soportado por herramientas y personal para responder a las consultas de los usuarios y administrar la resolución de incidentes. Sin embargo, se trata de un proceso no estandarizado y sólo se brinda soporte reactivo. La gerencia no monitorea las consultas de los usuarios, los incidentes o las tendencias. No existe un proceso de escalamiento para garantizar que los problemas se resuelvan

Administrar los datos: Se entiende y acepta la necesidad de la administración de datos, tanto dentro de TI como a lo largo de toda la organización. Se establece la responsabilidad sobre la administración de los datos. Se asigna la propiedad sobre los datos a la parte responsable que controla la integridad y la seguridad. Los procedimientos de administración de datos se formalizan dentro de TI y se utilizan algunas herramientas para respaldos / recuperación y desecho de equipo.

Administrar la configuración: La gerencia esta conciente de la necesidad de controlar la configuración de TI y entiende los beneficios de mantener información completa y precisa sobre las configuraciones, pero hay una dependencia implícita del conocimiento y experiencia del personal técnico. Las herramientas para la administración de

configuraciones se utilizan hasta cierto grado, pero difieren entre plataformas. Además no se han definido prácticas estandarizadas de trabajo.

Monitoreo y Evaluación

Monitorear y evaluar el desempeño de TI: La gerencia ha comunicado e institucionalizado un procesos estándar de monitoreo. Se han implantado programas educacionales y de entrenamiento para el monitoreo. Las evaluaciones todavía se realizan al nivel de procesos y proyectos individuales de TI y no están integradas a través de todos los procesos

Monitorear y evaluar el control interno: La organización utiliza reportes de control informales para comenzar iniciativas de acción correctiva. La evaluación del control interno depende de las habilidades de individuos clave. La organización tiene una mayor conciencia sobre el monitoreo de los controles internos. Los factores de riesgo específicos del ambiente de TI se identifican con base en las habilidades de individuos.

Garantizar el cumplimiento regulatorio: Se han desarrollado, documentado y comunicado políticas, procedimientos y procesos, para garantizar el cumplimiento de los reglamentos y de las obligaciones contractuales y legales, pero algunas quizá no se sigan y algunas quizá estén desactualizadas o sean poco prácticas de implementar.

Proporcionar gobierno de TI: Se reconoce que el tema del gobierno de TI existe y que debe ser resuelto. El enfoque de la gerencia es reactivo y solamente existe una comunicación esporádica e inconsistente sobre los temas y los enfoques para resolverlos. La gerencia solo cuenta con una indicación aproximada de cómo TI contribuye al desempeño del negocio.

6.3 *Determinar el nivel de madurez de cada objetivo de control*

De acuerdo con los resultados anteriores, en este paso el equipo determinó una calificación al comportamiento de cada objetivo de control diagnosticado, basado en los modelos de madurez definidos por COBIT para cada objetivo de control. Estos resultados se muestran en la tabla 3.2.

3.1.6. Etapa 7: Evaluación de la gestión de TI en la organización

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

El método utilizado para determinar los pesos fue el ANP de Saaty, los expertos asignaron la comparación pareada a partir de la escala de Saaty y teniendo en cuenta la red del indicador I_{GTI} construida en el Super Decission (Ver Anexo 5) se determinaron los pesos de los dominios y los objetivos de control. En las tablas 3.2 y 3.3 se ofrecen los pesos finales calculados en cada empresa.

7.2. *Evaluación de los dominios y objetivos de control*

La evaluación de los dominios (ED_g) y los objetivos de control (EOC_{dg}) se obtuvo a partir de las expresiones 2.4, 2.5 y 2.6. Los resultados se muestran en las tablas 3.2 y 3.3.

7.3. *Determinación del indicador I_{GTI}. Representación gráfica de los resultados*

De acuerdo con los resultados de las etapas anteriores se procedió a calcular el Indicador nivel de la gestión de TI (I_{GTI}) empleando la expresión 2.7. El indicador nivel de la gestión de TI en TECNOAZUCAR mostró un resultado de 49.3588% evaluándose la gestión de TI en un nivel 2: Repetible y en ATI de 55.2301% evaluándose la gestión de TI en un nivel 3: Definido.

En la figura 3.1 se muestran los radares de control para cada dominio. Es de destacar que en todos los dominios, los objetivos de control están de un nivel inicial en lo adelante, ninguno es evaluado de 0: no existente. En TECNOAZUCAR el dominio Adquisición e Implantación es el de peores resultados seguido por Monitoreo y Evaluación, en ATI el de peores resultados es Entrega y Soporte seguido por Planeación y Organización. En TECNOAZUCAR los objetivos de control de más bajo nivel evaluados fueron: Administrar recursos de TI, Administrar la calidad, Determinar la dirección tecnológica y Proporcionar gobierno de TI. Siendo en ATI Proporcionar gobierno de TI el de más baja evaluación.

Los radares correspondientes a los niveles de madurez de cada dominio se muestran en el Anexo 6 a) y b).

Tabla3.2. Pesos y evaluación de los dominios y objetivos de control en la empresa TECNOAZUCAR

	Objetivos de control	NM_{dg}	**Pesos**	EOC_{dg}	RD_g	ED_g **(%)**
Planificación y Organización			**0. 3488**		**0. 50084**	**17. 46929**
	Definir el plan estratégico de TI.	3	0. 2105	0. 1263		
	Definir la arquitectura de la información.	3	0. 1261	0. 07566		
	Determinar la dirección tecnológica.	1	0. 0724	0. 01448		
	Definir los procesos, organización y relaciones de TI.	3	0. 2457	0. 14742		
	Comunicar las aspiraciones y la dirección de la gerencia.	3	0. 0576	0. 03456		
	Administrar los recursos humanos de TI	2	0. 0518	0. 02072		
	Administrar la calidad	1	0. 0633	0. 01266		
	Evaluar y administrar los riesgos de TI	2	0. 1726	0. 06904		
Adquisición e Implantación			**0. 1361**		**0. 46304**	**6. 30197**
	Identificar soluciones automatizadas.	2	0. 0494	0. 01976		
	Adquirir y mantener la infraestructura tecnológica	3	0. 0679	0. 04074		
	Facilitar la operación y el uso	3	0. 1669	0. 10014		
	Administrar recursos de TI	1	0. 2013	0. 04028		
	Administrar cambios.	3	0. 2818	0. 16908		
	Instalar y acreditar soluciones y cambios	2	0. 2326	0. 09304		
Entrega y Soporte			**0.2149**		**0.63376**	**13.61950**
	Administrar los servicios de terceros	3	0. 1100	0. 066		
	Administrar el desempeño y la capacidad de TI	2	0. 0245	0. 0098		
	Garantizar la continuidad del servicio.	4	0. 1420	0 .1136		
	Garantizar la seguridad de los sistemas.	3	0. 1429	0. 08574		
	Educar y entrenar a los usuarios.	3	0. 1909	0. 11454		
	Administrar la mesa de servicios y los incidentes.	3	0. 2235	0. 1341		
	Administrar la configuración.	3	0. 1059	0. 06354		
	Administrar los datos.	4	0. 0513	0. 04104		
	Administrar el ambiente físico	3	0. 0090	0. 0054		
Monitoreo y Evaluación			**0. 3001**		**0. 3988**	**11. 96799**
	Monitorear y evaluar el desempeño de TI	2	0. 5611	0. 22444		
	Monitorear y evaluar el control interno	2	0. 3415	0. 1366		
	Garantizar cumplimiento regulatorio	3	0. 0457	0. 02742		
	Proporcionar gobierno de TI	1	0. 0517	0. 01034		

Tabla 3.3. Pesos finales y evaluación de los dominios y objetivos de control de ATI

	Objetivos de control ATI	*NM*	Pesos	EOC_{dg}	RD_g	ED_g (%)
Planificación y Organización			**0. 1784**		**0. 55346**	**9. 87373**
	Definir el plan estratégico de TI.	3	0. 3039	0. 18234		
	Definir la arquitectura de la información.	2	0. 0925	0. 037		
	Determinar la dirección tecnológica.	2	0. 0455	0. 0182		
	Definir los procesos, organización y relaciones de TI.	3	0. 1001	0. 06006		
	Administrar la inversión de TI	2	0. 0362	0. 01448		
	Comunicar las aspiraciones y la dirección de la gerencia	3	0. 0168	0. 01008		
	Administrar la calidad	4	0. 1359	0. 10872		
	Evaluar y administrar los riesgos de TI	3	0. 0747	0. 04482		
	Administrar proyectos	2	0. 1944	0. 07776		
Adquisición e Implantación			**0. 2829**		**0. 53682**	**15.18664**
	Identificar soluciones automatizadas.	3	0. 1608	0. 09648		
	Adquirir y mantener software aplicativo	3	0. 1482	0. 08892		
	Adquirir y mantener la infraestructura tecnológica	3	0. 0539	0. 03234		
	Facilitar la operación y el uso	2	0. 1489	0. 05956		
	Administrar recursos de TI	3	0. 0907	0. 05442		
	Administrar cambios.	3	0. 2305	0. 1383		
	Instalar y acreditar soluciones y cambios	2	0. 1670	0. 0668		
Entrega y Soporte			**0. 1445**		**0. 60486**	**8.74023**
	Definir y administrar niveles de servicio	3	0. 1144	0. 06864		
	Administrar los servicios de terceros	3	0. 1869	0. 11214		
	Administrar el desempeño y la capacidad de TI	3	0. 0595	0. 0357		
	Garantizar la continuidad del servicio.	4	0. 1681	0. 13448		
	Garantizar la seguridad de los sistemas.	4	0. 1134	0. 09072		
	Educar y entrenar a los usuarios.	3	0. 0712	0. 04272		
	Administrar la mesa de servicios y los incidentes.	2	0. 2221	0. 08884		
	Administrar la configuración.	2	0. 0351	0. 01404		
	Administrar los datos.	3	0. 0293	0. 01758		
Monitoreo y Evaluación			**0. 3942**		**0. 54362**	**21. 42950**
	Monitorear y evaluar el desempeño de TI	3	0. 7368	0. 44208		
	Monitorear y evaluar el control interno	2	0. 1729	0. 06916		
	Garantizar cumplimiento regulatorio	3	0. 0358	0. 02148		
	Proporcionar gobierno de TI	1	0. 0545	0. 0109		

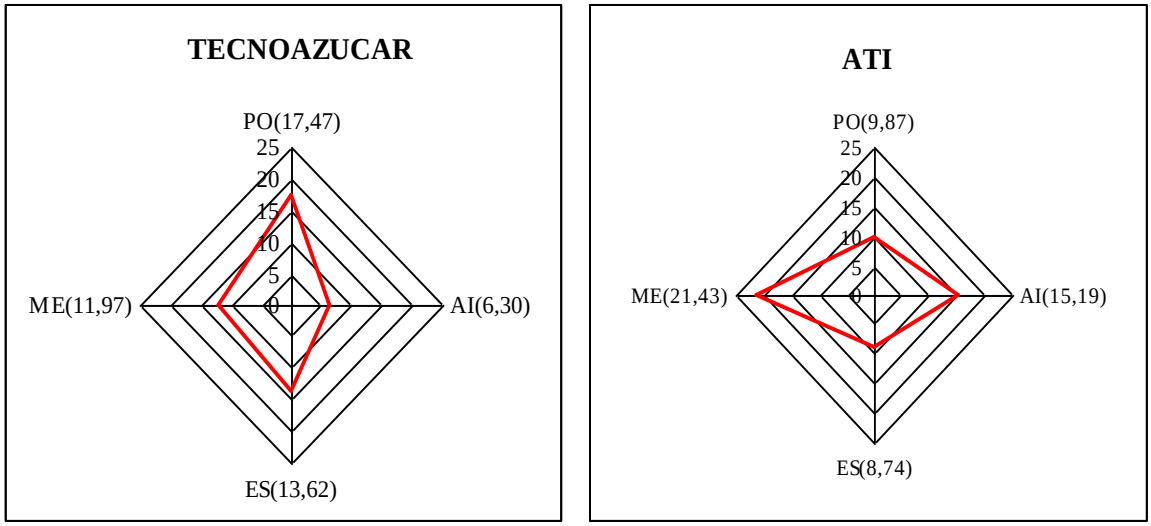


Figura 3.1. Radares de control de los dominios en cada empresa.

7.4. *Elaboración del informe de evaluación*

A partir del análisis de los resultados anteriores, el equipo de trabajo elaboró un informe de evaluación señalando los principales problemas que afectan la gestión de TI en las empresas, los que se muestran a continuación. Se graficó en dos diagramas Causa – Efecto mostrados en las figuras 3.2 y 3.3.

TECNOAZUCAR

- No existe un plan de infraestructura tecnológica que establezca y administre las expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación.
- La función de TI no se encuentra en la estructura organizativa de la empresa.
- Análisis de riesgos poco abarcador.
- No se mide la calidad de los servicios de TI.
- No existe un enfoque formal y continuo con respecto a la administración de la calidad.
- No existe una metodología, ni se tienen en cuenta parámetros para verificar que las soluciones se ajustan al propósito deseado.
- No se administra de manera rigurosa la prestación de servicios de terceros
- No se tienen establecidos indicadores de continuidad y seguridad de los servicios de TI.
- Insuficiente administración de la configuración específica de los sistemas.

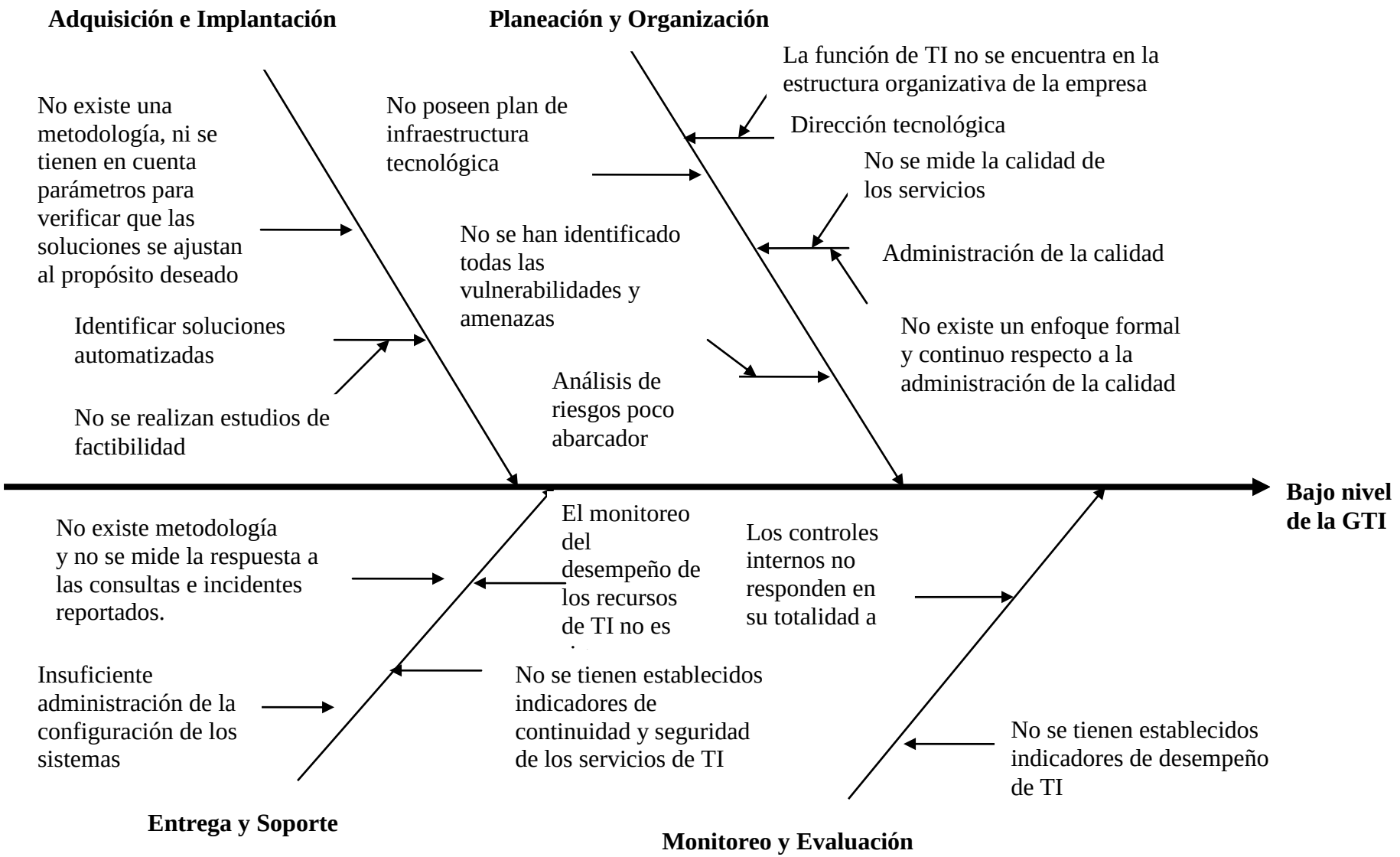


Figura 3.2. Principales problemas de la gestión de TI en la empresa TECNOAZUCAR

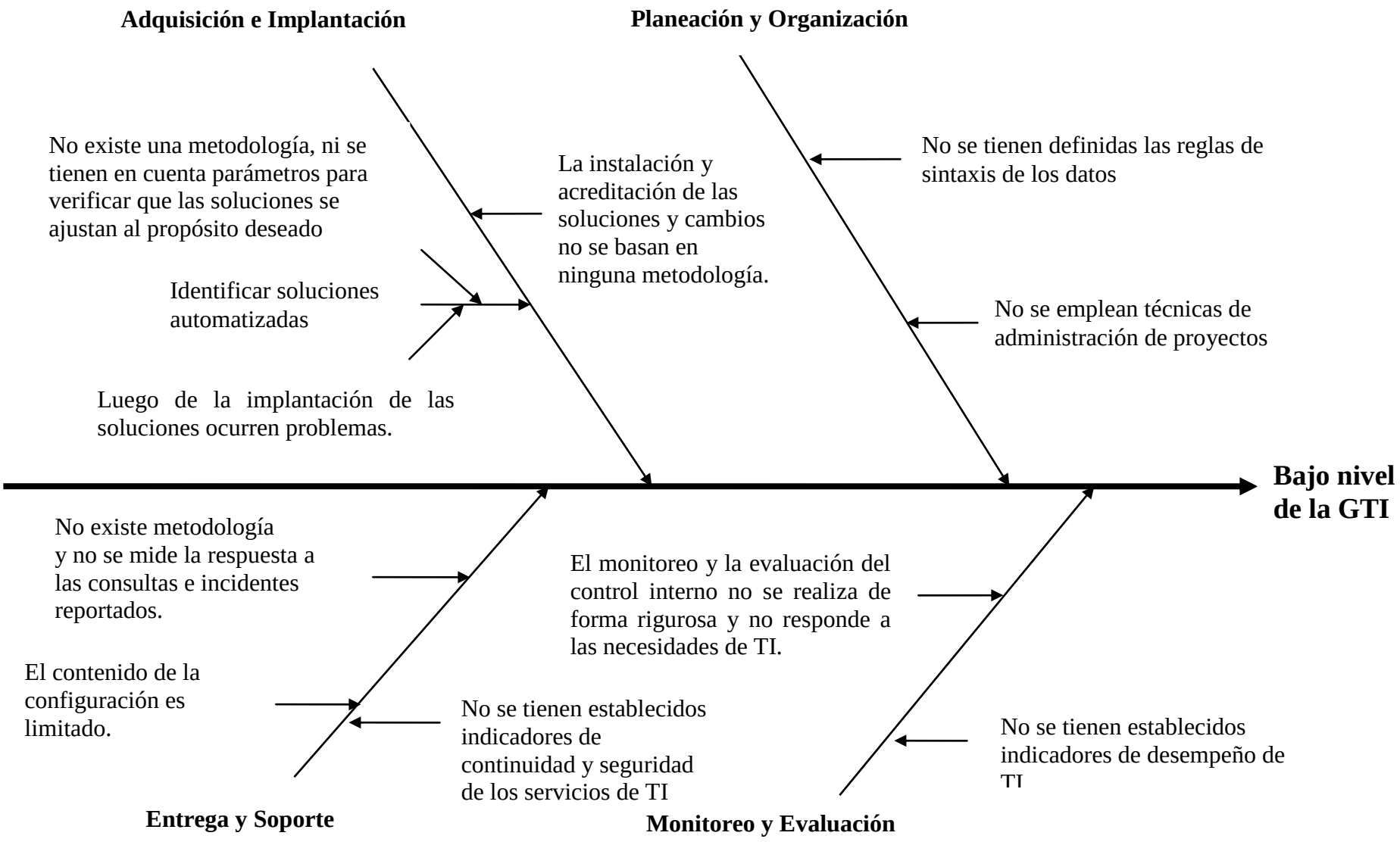


Figura 3.3. Principales problemas de la gestión de TI en la empresa ATI

- No existe una metodología y no se mide la respuesta a las consultas e incidentes reportados.
- No se tienen establecidos indicadores de desempeño de TI relevantes.
- Los controles internos no responden en su totalidad a las necesidades de las TI.

ATI

- No se tienen definidas las reglas de sintaxis de los datos.
- No se emplean técnicas de administración de proyectos.
- No existe una metodología para verificar que las soluciones se ajusten al propósito deseado.
- Luego de la implantación de las soluciones ocurren problemas.
- La instalación y acreditación de las soluciones y cambios no se basan en ninguna metodología.
- No se mide la respuesta a las consultas e incidentes reportados
- No se tienen establecidos indicadores de continuidad y seguridad de los servicios de TI.
- El contenido de la configuración es limitado.
- No se tienen establecidos indicadores de desempeño de TI relevantes
- El monitoreo y la evaluación del control interno no se realiza de forma rigurosa y no responde a las necesidades de TI.

3.1.7. Etapa 8: Propuesta de medidas correctivas, preventivas y/o de mejora

A partir de la etapa anterior se proponen una serie de medidas que ayudaran a la mejora de la GTI en cada empresa.

TECNOAZUCAR

- Establecer un plan de infraestructura tecnológica que establezca y administre las expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación.
- Realizar un análisis más profundo respecto a los riesgos incluyendo todas las vulnerabilidades presentes y posibles amenazas.

– Incluir la función de TI en la estructura organizativa de la empresa.

– Medir la calidad de los servicios de TI.

– Establecer un enfoque formal y continuo con respecto a la administración de la calidad.

– Establecer una metodología y parámetros que verifiquen que las soluciones se ajustan al propósito deseado de la entidad.

– Establecer indicadores de continuidad y seguridad de los servicios de TI.

– Establecer una línea base de elementos de configuración específica para cada sistema y servicio.

– Establecer una metodología y medir la respuesta a las consultas e incidentes reportados.

– Establecer indicadores de desempeño de TI relevantes así como identificar e implementar acciones de mejoramiento del desempeño

– Mejorar el monitoreo y la evaluación de los controles internos para que respondan a las necesidades de las TI y se satisfagan los objetivos de la empresa y de las TI.

– Identificar acciones de mejoramiento para el control interno

ATI

– Definir las reglas de sintaxis de los datos según las necesidades de la empresa.

– Emplear técnicas de administración de proyectos que permitan tomar decisiones oportunas.

– Establecer una metodología y parámetros que verifiquen que las soluciones se ajustan al propósito deseado de la entidad.

– Establecer una metodología de prueba que garantice pruebas de aceptación suficientes antes de liberar el cambio.

– Realizar de forma regular análisis de tendencias de incidentes y consultas

– Establecer indicadores de continuidad y seguridad de los servicios de TI.

– Identificar todos los elementos de configuración y mantener la información de la configuración.

– Establecer indicadores de desempeño de TI relevantes así como identificar e implementar acciones de mejoramiento del desempeño

– Mejorar el monitoreo y la evaluación de los controles internos para que respondan a las necesidades de las TI y se satisfagan los objetivos de la empresa y de las TI.

3.2. Conclusiones parciales

1. Con la aplicación del procedimiento general en las empresas TECNOAZUCAR y ATI se pudo determinar los problemas que afectan la gestión de las TI en esta empresa, resultando que los dominios con peor evaluación fueron Adquisición e Implantación y Entrega y Soporte respectivamente.

2. A través del cálculo del indicador propuesto IGTI, es posible evaluar la gestión de TI. Al calcular el indicador en ambas empresas objetos de estudio, se obtuvieron los resultados del 49.3588% 55.2301% evaluándose entonces la gestión de TI de nivel 2 Repetible en TECNOAZUCAR y nivel 3: Definido para ATI.

3. El procedimiento general para el diagnóstico de la gestión de las TI arrojó que las principales dificultades de la gestión de TI en TECNOAZUCAR se centran en la no existencia de un plan de infraestructura tecnológica, en no contar con una administración de la calidad, no tener establecidos parámetros para la adquisición de recursos de TI y en ATI no se tienen definidas las reglas de sintaxis de los datos, no existe una metodología para verificar que las soluciones se ajusten al propósito deseado, la instalación y acreditación de las soluciones y cambios no se basan en ninguna metodología.

Conclusiones generales

1. La bibliografía utilizada para la construcción del marco teórico - referencial de la investigación confirma la presencia de una abundante base teórica conceptual sobre la gestión de las TI así como lo importante que es para una empresa la evaluación de la misma. Sin embargo son muy escasos los precedentes en la bibliografía consultada de procedimientos e indicadores que permitan diagnosticar el estado actual de la gestión de TI en una organización, por lo cual se seleccionó el procedimiento propuesto por Pérez Lorences (2010), que considera la alineación de TI a los objetivos de negocio y la administración de los riesgos y beneficios asociados.

2. Al analizar la situación problemática fundamentada en esta investigación se demostró la necesidad de aplicar el procedimiento general para el diagnóstico de la gestión de las TI en las empresas UEB TECNOAZÚCAR y ATI de Villa Clara, con vistas a su mejora para garantizar que las TI soporten las metas del negocio y de esta forma contribuir al desarrollo de un enfoque de mejora continua hacia la competitividad empresarial. Esto corroboró la correcta formulación del problema científico planteado en la tesis.

3. El cálculo del indicador integral I_{GTI} reveló que la gestión de TI en la UEB TECNOAZÚCAR está en el nivel 2 Repetible y en el caso de la empresa ATI en nivel 3 Definido. El comportamiento de la gestión de TI difiere significativamente en ambas empresas, mientras para TECNOAZÚCAR los dominios peores evaluados fueron "Adquisición e Implantación" seguido de "Monitoreo y Evaluación"; para ATI fueron "Entrega y Soporte" y "Planificación y Organización". Se destacan como problemas comunes los objetivos de control: Determinar la dirección tecnológica, Instalar y acreditar soluciones y cambios, Monitorear y evaluar el control interno, y Proporcionar gobierno de TI.

4. La aplicación del procedimiento propuesto por Pérez Lorences (2010) en las dos empresas objeto de estudio, permitió el análisis de la alineación de los recursos de TI a los objetivos de negocio, la determinación de los problemas que afectan la gestión de las TI, la evaluación de dicha gestión a través de un indicador integral, así como la determinación de oportunidades de mejora. Todo esto permitió validar la hipótesis formulada en esta investigación.

Recomendaciones

1. Continuar el desarrollo de la investigación en las empresas objeto de estudio, a partir de la implementación de las propuestas de mejora, que pueden resumirse en el diseño e implementación de un proceso de gestión de TI que permita a las empresas formalizar sus actividades al respecto y monitorear adecuadamente el uso de tan valiosos recursos.

2. Aplicar el procedimiento utilizado en la investigación para el diagnóstico de la gestión de TI en otras empresas, valiéndose de los principios de flexibilidad y generalidad sobre los que se sustenta el mismo, para contribuir al mejoramiento de la gestión de TI en otras organizaciones.

Bibliografía

1. Arias, M., (2009) *Procedimiento de diagnóstico de la gestión de tecnologías de la información. Aplicación en la empresa Desoft V.C.* Trabajo de Diploma. Cuba, Departamento de Ingenieria Industrial y Turismo, Universidad Central Martha Abreu de las Villas
2. Berea, D. C. (2006). Gestión de Servicios de TI: ITIL e ISO 20000. ITE Caixa Galicia
3. Borousan, E et al., (2011). "Balanced Scorecard; a Tool for Measuring and Modifying IT Governance in Healthcare O-rganizations" en *International Journal of Innovation, Management and Technology*, Vol. 2, No. 2, April 2011, pp 141-146
4. Caporarello, L. (2008). IT Governance: A framework proposal, and empirical study. Thesis submitted for the degree of the XX Doctor of Philosophy in Management Information Systems at LUISS University. Rome. Italy
5. COBIT4.1. (2007). Control Objectives for Information and related Technology. Disponible en http:// www.itgi.org/COBIT.htm.
6. Colectivo de autores. (2005). Alining COBIT, ITIL an ISO 17799 for Business Benefit. s.l. Disponible en: http://www.itgi.org
7. Colectivo de autores (2008). Directrices de Auditoría. Disponible en www.unap.cl/~setcheve/ati/LinkedDocuments/DIRECTRICES_DE_AUDITORIA
8. Corona, M., (2010). "Alineación TI/Negocio, ventajas competitivas y procesos de ITIL". *Pink Elephant – ¡Celebrando 20 años de experiencia en ITIL! Disponible en: www.pinkelephant.com*
9. Espinosa B, G E., (2011) "BSM como Estrategia de Integración de las TI al Negocio" en *Revista Iberoamericana de Sistemas, Cibernética e Informática* [En línea], Venezuela, Disponible en: http:// *www.iiisci.org/journal/risci/*
10. Fernández, J; Mayol, E; Pastor, JA., (2011). "Agile Business Intelligence Governance: Su justificación y presentación". *ITGSM VI Congreso Académico*

Internacional en Gobierno TI y Gestión del servicio. itsmf, 2011, Barcelona, Catalunya, disponible en: *www.uc3m.es/portal/page/portal/congresos_jornadas/itgsm_2011*

11. Gómez, C de Oro., (2010) "La Gestión de Riesgo de TI en el Marco Corporativo" en *SIC* [En línea],. No 88, febrero 2010,pp 54[Accesado el 3 de marzo de 2012]
12. Gómez, RC; Martínez, C (2008) "Implementación de Gobierno de Tecnologías de Información y Comunicaciones (TICs) en la Empresa".*Buenas Tareas*, Cuba. Disponible en: http://www.buenastareas.com
13. Henderson & Venkatraman (1993). Strategic alignment: leveraging information technology for transforming organizations. *IBM Systems Journal*, Vol. 32
14. IBM. , (2008) "Gobierno de TI: obtener el máximo rendimiento en los momentos críticos" en *IBM España* [En línea], junio 2008, Madrid, disponible en: ibm.com. [Consultado en marzo, 3, 2012]
15. IBM. , (2009) "Gestión de riesgos de TI: Unos sistemas de información maduros pueden generar grandes resultados" en *IBM España*[En línea], enero 2009, Madrid, disponible en: www.ibm.com/es [Consultado en marzo, 3, 2012]
16. ISO/IEC 20000-1 (2005) Information technology -- Service management -- Part 1: Specification. Disponible en: http://www.iso.org/iso/catalogue
17. ISO/IEC 20000-2 (2005) Information technology -- Service management -- Part 2: Code of practice. Disponible en: http://www.iso.org/iso/catalogue
18. ISO/IEC 27001 (2005) Information technology - Security techniques - Information security management systems – Requirements. Disponible en: http://www.iso.org/iso/catalogue
19. ISO/IEC 27002 (2005). Information technology -- Security techniques -- Code of practice for information security management. Disponible en: http://www.iso.org/iso/catalogue
20. ISO/IEC 27005 (2008). Information technology -- Security techniques -- Information security risk management. Disponible en: http://www.iso.org/iso/catalogue

21. ISO/IEC 38500 (2008). Corporate Governance of Information Technology. . Disponible en: http://www.iso.org/iso/catalogue
22. ITGI., (2007) "Implementation GuideUsing COBIT® and Val IT". [En línea],*itgi.org* , Estados Unidos, disponible en: www.itgi.org
23. ITGI. (2009)., "Enables IS0/IEC 38500:2008 Adoption". [En línea], *itgi.org*, Estados Unidos, disponible en: www.itgi.org
24. ITGI and OGC., (2008) "Aligning CobiT® 4.1, ITILG® V3 and ISO/IEC 27002 for Business Benefit".[En línea], *itgi.org*, Estados Unidos e Inglaterra, disponible en: www.itgi.or
25. ITIL. (2006). Versión 2. s.l.: Disponible en: http://www.itil.co.uk, 2006. Disponible en: http://www.symantec.com,
26. ITIL. (2007). Versión 3. s.l.: Disponible en: http://www.itil.co.uk.
27. IT Risk Management Report Volumen 2: Myths and realities (2008). Symantec. Trends through December 2007. Disponible en: http://www.symantec.com
28. itSMF. (2005). Metodologías y marcos de referencia en Gestión de Servicios de TI. Argentina. Disponible en: http://www.itsmf-argentina.com.ar, 2005.
29. Kaplan, R., Norton, D. (2001). The Strategy Focused Organization. Cómo utilizar el Cuadro de Mando Integral, para implementar y gestionar su estrategia. Ediciones Gestión 2000
30. López Paz, C. (2009). "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 2009. Disponible en: http://www.informaticahabana.cu/
31. López Paz, C et al.., (2010) "Servicios Especializados de Consultoría TI para alinear componentes de negocio y componentes TI en organizaciones manufactureras". JDARE 2010 Jornada para el desarrollo de Grandes Aplicaciones de Red Universidad de Alicante, España, pp 309-406
32. Luna, A. J. H. de O. et al .,(2010) **"**Agile Governance in Information and Communication Technlogies: Shifting Paradigms G" en *Journal of Information*

Systems and Technology Management [En línea], Vol. 7, No. 2, 2010, TECSI FEA USP – 2010 Universidade Federal de Pernambuco, Brasil.

33. Marcos Pascual, F. (2005). Gestión de TI. Disponible en www.econsultia.es/images/news /documentacion
34. Maxitana Cevallos, J. (2005). Administración de riesgos de tecnología de la información de una empresa del sector informático. Tesis. Instituto de Ciencias Matemáticas, Escuela Superior Politécnica del Litoral. Ecuador.
35. Meyer, S., (2007*) BUSINESS SERVICE MANAGEMENT: Fusión de los servicios de TI y los objetivos empresariales: BUSINESS SERVICE MANAGEMENT*. CA, Empresas de software de gestión de tecnologías de la información
36. NIST Special Publication 800-30. (2002). Risk Management Guide for Information Technology Systems. *Recommendations* of the National Institute of Standards and Technology.
37. Pathak, Jagdish (2005). "Information Technology Auditing" Odette, *Springer Science+Business* Media, Alemania, disponible en: springeronline.com
38. Pérez Lorences, P. (2010). *Procedimiento para evaluar y mejorar la gestión de tecnologías de la información en empresas cubanas.* Tesis presentada en opción al título académico de máster en informática empresarial. Santa Clara. Universidad Central Martha Abreu de las Villas
39. Pérez Sánchez, A. (2008). "ISO/IEC 20000 el estándar para la Gestión de Servicios TI"
40. Kaplan , R , Norton, D. (2001). The Strategy Focused Organization. Cómo utilizar el Cuadro de Mando Integral, para implementar y gestionar su estrategia. Ediciones Gestión 2000
41. Reyes Retana, G. (2006). Panorama general de la Administración de Servicios ITIL. Disponible en: http://www.pinkelephant.com
42. Salazar, C; Lam, J. (2011) *La Informática y su impacto social.* Monografía. Institución: Universidad de Pinar del Río "Hermanos Saíz Montes de Oca. Cuba.

Disponible en: http://www.monografias.com/trabajos14/informatica-social/informatica-social.shtml

43. Sánchez Hilara E. (2008). Indicadores de evaluación de la calidad de los servicios TI. Auditoría y Seguridad, No22, 28, 29.
44. The Risk IT Framework (2009). Enterprise Risk: Identify, Govern and Manage IT Risk. Risk IT based on COBIT. IT Governance Institute. Disponible en http://www.itgi.org
45. Van Grembergen, W. (2002). *Introduction to the Minitrack IT Governance and Its Mechansims*, Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS), 2002
46. Vam Grembergen (ed), (2004) "Strategies for Information Technology Governance", Estados Unidos, disponible en:http://www.idea-group.com
47. Van Grembergen, W. (2007). The Balanced Scorecard and IT Governance. Information Systems Control Journal. Reprinted by IT Governance Institute™
48. Van Grembergen, W. & De Haes, S. (2009) Enterprise Governance of Information Technology. Achieving Strategic Alignment and Value. Springer e-ISBN 978-0-387- 84882-2.

Anexo 1. Tabla resumen de conceptos de gobierno de TI.

Autores	Conceptos
Marrón y Magill (1994)	El gobierno de TI describe el punto de la responsabilidad para las funciones de TI.
Luftman (1996)	El gobierno de TI es la autoridad para lo lograr las decisiones de la dirección respecto a las TI y fijar las prioridades de TI y la asignación de recursos de TI.
Sambamurthy y Zmud (1999)	El gobierno de TI consulta las estructuras de la autoridad para las actividades de TI.
Van Grembergen (2002)	El gobierno de TI es la capacidad organizativa de la dirección y los ejecutivos controlar la formulación y la puesta en práctica de la estrategia de TI y de este modo asegurar la fusión de empresa y las TI.
Weill y Vitale (2002)	El gobierno de TI describe el proceso en conjunto para compartir la decisión de los derechos sobre la TI y monitorear el rendimiento de inversiones de TI.
Schwarz y Hirschheim (2003)	El gobierno de IT consta de las estructuras de las arquitecturas de TI, para implementar con éxito y lograr las actividades de TI en respuesta a al ambiente estratégico en la empresa
Instituto de Gobierno de TI (2004)	El gobierno de TI es la responsabilidad de los directorios y los ejecutivos de dirección. Es parte esencial del gobierno de la empresa y consta del liderazgo y las estructuras organizativas y los procesos que aseguran que las TI de la organización sostengan y extiendan las estrategias y los objetivos de la organización.
Weill y Ross (2004)	El gobierno de TI está especificando los derechos de decisión y la rendición de cuentas en base de apoyar el comportamiento deseable en el uso de las TI.
COBIT (2007)	Gobierno de TI es el aseguramiento del valor de TI, la administración de los riesgos asociados a las TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave de la gestión de la empresa.
ITGI, 2008; ISACA, 2007; ITSMF, 2008	Gobierno de TI es como un subconjunto de la disciplina de gobierno corporativo o de la empresa, que se concentra en la TI y sus sistemas de rendimiento y en la prevención de riesgos

Guía de entrevista para el dominio Planificación y Organización.

Definir el plan estratégico de TI.

- ¿Existe un plan estratégico de TI?
- ¿Se identifican las áreas que dependen de forma crítica de TI?
- ¿Se evalúa el desempeño de los recursos de TI en términos de su contribución a los objetivos de negocio?
- ¿Cómo se realiza la planeación estratégica de TI?

Definir la arquitectura de la información

- ¿Se ha definido la arquitectura de la información de la empresa?
- ¿Está definidas las reglas de sintaxis de los datos de la organización?
- ¿Existe un esquema de clasificación de datos?
- ¿Están definidos niveles de seguridad de los datos?

Determinar la dirección tecnológica.

- ¿Existe un plan de infraestructura tecnológica?
- ¿Están definidos planes de adquisición, estrategias de mitigación y contingencias?
- ¿Se monitorean las tendencias tecnológicas, de infraestructura, legales y regulatorias?

Definir procesos, organización y relaciones de TI.

- ¿Está ubicada la función de TI en la estructura organizacional de la empresa?
- ¿Cuál es la estructura organizacional de TI?
- ¿Existen roles y responsabilidades definidas para la organización de TI?

Administrar la inversión en TI.

- ¿Cómo se administra la inversión en TI?
- ¿Se mide el ROI de las inversiones en TI?
- ¿Cómo se planifica el presupuesto de TI?

Comunicar las aspiraciones y la dirección de la gerencia.

- ¿La dirección define políticas, procedimientos, directrices y otra documentación para controlar las TI?

Administrar recursos humanos de TI.

- ¿Cómo se administran los recursos humanos de TI?
- ¿Se imparte entrenamiento al personal nuevo de TI?
- ¿Se asignan roles en correspondencia con las habilidades?
- ¿Se minimiza la dependencia de individuos?
- ¿Cómo se evalúa el desempeño del personal de TI?

Administrar calidad.

- ¿Se mide la calidad de los servicios de TI?
- ¿Existe un enfoque formal y continuo con respecto a la administración de la calidad?
- ¿Se revisa la calidad de los proyectos y las operaciones de TI?

Evaluar y administrar riesgos

- ¿Se identifican los eventos con un impacto potencial sobre las metas de la organización?
- ¿se evalúan los riesgos de TI?
- ¿Existe un plan de acción de riesgos?

Administrar proyectos

- ¿se emplean técnicas de administración de proyectos en los proyectos de TI?

- ¿cómo se administran los proyectos de TI?

Guía de entrevista para el dominio Adquisición e Implantación.

Identificar soluciones automatizadas.

- ¿Cómo se analizan las necesidades de nuevas aplicaciones o funciones para satisfacer requisitos de negocio en su empresa?
- ¿Se realizan estudios de factibilidad para las soluciones identificadas? ¿Qué tienen en cuenta?
- ¿Existe una metodología establecida para la identificación y evaluación de las soluciones de TI?

Adquirir y mantener el software aplicativo.

- ¿Cómo se lleva a cabo la compra y/o mantenimiento de los software aplicativos y basados en que parámetros?
- ¿Existe algún procedimiento definido? ¿Qué contempla?

Adquirir y mantener la infraestructura tecnológica

- ¿Cómo se realiza la adquisición y mantenimiento de la infraestructura tecnológica?
- ¿Cuáles son los parámetros a tener en cuento para adquirir las infraestructuras tecnológicas?
- ¿Cómo se planifica y se lleva a cabo el mantenimiento de las infraestructuras?

Facilitar la operación y el uso.

- ¿Existen manuales efectivos de usuarios para la operación y el uso exitoso de los sistemas?
- ¿Se realiza algún tipo de entrenamiento en la empresa para los usuarios de los servicios brindados? ¿Esporádicamente o con frecuencia fija?
- ¿Existe alguna documentación donde esté plasmado los entrenamientos que se les proporcionan a los usuarios?
- ¿El material y programa de entrenamiento es actualizado?

Adquirir recursos de TI.

- ¿La adquisición de recursos de TI forma parte del proceso de adquisición de la empresa?
- ¿Existen procedimientos definidos para la adquisición de recursos de TI? ¿Cómo se realiza esta adquisición?
- ¿Qué parámetros se tienen en cuenta?

Administrar cambios.

- ¿Existe algún documento o procedimiento que estipule lo que ha de hacerse en caso de realizarse algún cambio (incluyendo mantenimientos y parches)? ¿Qué plantea?
- ¿Estos cambios se realizan bajo la autorización y responsabilidad de una persona definida?

Instalar y acreditar soluciones y cambios.

- ¿Se verifica que las soluciones se ajusten al propósito deseado?
- ¿Existe alguna metodología para ello o se realiza bajo la iniciativa de alguien?
- ¿Existen problemas posteriores a la implementación de las soluciones? ¿Cómo cuáles?

Guía de entrevista para el dominio Entrega y Soporte.

Definir y administrar niveles de servicio.

- ¿Se definen acuerdos de niveles de servicio (SLA)?

- ¿Los SLA se monitorean periódicamente y se reevalúan?
- ¿Se tiene en cuenta la satisfacción del cliente? ¿Cómo se mide esta?

Administrar servicios de terceros.

- ¿Cómo se administra la prestación de servicios de terceros?
- ¿Bajo qué parámetros, documentación o proceso?
- ¿Cómo se seleccionan los proveedores de servicios?

Administrar el desempeño y la capacidad.

- ¿Se monitorea el desempeño y la capacidad de los recursos de TI para garantizar que soporten los requerimientos del negocio?
- ¿Se pronostica el desempeño y la capacidad de los recursos de TI para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño?

Garantizar la continuidad del servicio.

- ¿Existe algún plan para garantizar la continuidad del servicio y reducir el impacto de las interrupciones?
- ¿Se identifican los recursos críticos para priorizar la recuperación del servicio?
- ¿El plan de continuidad está documentado y basado en la criticidad de los sistemas y el impacto al negocio?

Garantizar la seguridad de los sistemas.

- ¿Los requerimientos de seguridad de TI están documentados?
- ¿Las responsabilidades sobre la seguridad están asignadas, entendidas e implementadas?
- ¿Existen procedimientos de seguridad definidos? ¿Se define un plan de seguridad de TI?
- ¿Se realiza la capacitación en seguridad para TI y para el negocio?

Identificar y asignar costos.

- ¿Cómo se asignan los costos de TI?
- ¿La distribución de los costos de TI está identificada?
- ¿Existe un modelo definido y documentado de costos de servicios de información?

Entrenar y educar a los usuarios.

- ¿Se identifican las necesidades de entrenamiento de los diferentes grupos de usuarios?
- ¿Existe algún programa definido para la impartición de entrenamientos y educación?
- ¿Se evalúan los resultados de los entrenamientos realizados?

Administrar la mesa de servicios y los incidentes.

- ¿Existen una función de "mesa de servicio" definida para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información?
- ¿Se mide la respuesta oportuna a las consultas e incidentes reportados?
- ¿Conocen los usuarios dónde y cómo reportar problemas e incidentes?

Administrar la configuración.

- ¿Se establece una línea base de elementos de configuración para cada sistema y servicio?
- ¿Están documentados y estandarizados procedimientos para realizar la administración de la configuración?
- ¿Se revisa y verifica regularmente el status de los elementos de configuración?

Administración de problemas.

- ¿Se definen cuales son los problemas existentes?
- ¿Cómo los resuelven y quién o quiénes son los responsables?
- ¿Los métodos y procedimientos están documentados y estandarizados?

Administración de datos.

- ¿La información está disponible cuando se necesita?
- ¿Los datos son protegidos y cuentan con respaldo, recuperación y desecho?
- ¿Existe algún tipo de entrenamiento respecto a la administración de datos?

Administración de ambiente físico.

- ¿Se implementan y monitorean los controles ambientales?
- ¿Se les da mantenimiento a las instalaciones?
- ¿Se regula el personal que se mueve dentro de estas?
- ¿El mantenimiento y el control de personal está estandarizado y documentado?

Administración de operaciones.

- ¿Existe algún documento o proceso donde esté plasmado las operaciones de cómputo?
- ¿Estas operaciones son del conocimiento de todo el personal?
- ¿Se producen demoras o paros debido al desconocimiento de las operaciones a seguir?
- ¿El mantenimiento está programado y estipulado?

Guía de entrevista para el dominio Monitoreo y Evaluación.

Monitorear y evaluar el desempeño de TI.

- ¿Cómo y cuando se realiza el seguimiento y la evaluación de las aplicaciones, sistemas y procesos?
- ¿Este proceso o procedimiento está documentado y estandarizado?

Monitorear y evaluar el control interno.

- ¿Se llevan a cabo controles internos? ¿Estos están programados?
- ¿Responden a las necesidades de las TI o se encuentran implícito en algún otro tipo de control?
- ¿A través de que herramientas se lleva a cabo?

Garantizar cumplimiento regulatorio.

- ¿Se conoce y cumple con los requisitos regulatorios contractuales y legales de TI? ¿Cómo se garantiza este cumplimiento?
- ¿El conocimiento es general o de algunos individuos en específico?

Proporcionar gobierno de TI.

- ¿Conoce lo que es gestión de TI?
- ¿Se lleva a cabo en su empresa de manera formal?

¿Es considerada como una ventaja competitiva?

Anexo 3 a) Clasificación de los recursos en la empresa TECNOAZUCAR

No	RECUR-SOS	CLASIFI-CACIÓN			TECNOAZUCAR DESCRIPCIÓN	PROCESO	IMPAC-TO		
		A	I	P			F	M	D
1	Cl (HANEL)		X		M. Board Intel d 201 GL8, Procesador Intel Celeron 1.33Ghz, RAM 256MB (DDR 2)	Dirección	X		
2	Cl (HANEL)		X		M. Board Intel d 201 GL8, Procesador Intel Celeron 1.33Ghz, RAM 256MB (DDR 2)	Dirección			X
3	LTEL		X		M. Board P5 VD2-Vm, Procesador Celeron D-3.06 Ghz RAM 256MB (DDR 2)	Dirección			X
4	LTEL		X		M. Board P5 VD2-Vm, Procesador Celeron D-3.06 Ghz RAM 256MB (DDR 2)	Sala de análisis	X		
5	AOPEN		X		M. Board Intel DG41 CN, Procesador Dual Core 1.86Ghz, RAM 1GB (DDR2)	Logística	X		
6	AOPEN		X		M. Board Mx3W-Pro, Procesador Celaron 400 Mhz Memoria RAM 128 MB(DIMM)	Logística		X	
7	Cl (HANEL)		X		M. Board Intel d 201 GL8, Procesador Intel Celeron 1.33Ghz, RAM 256MB (DDR 2)	Logística		X	
8	HANEL		X		M. Borrad Intel d101 GGE, Procesador Intel Celeron 2.66Ghz, RAM 256MB (DDR1)x	Grupo técnico		X	
9	Cl (HANEL)		X		M. Board xIntel d 201 GxL8, Procesador Intel Celeron 1.33Ghz, RAM 256MB (DDR 2)	Grupo técnico		X	
10	Cl (HANEL)		X		M. Board Intel d 201 GL8, Procesador Intel Celeron 1.33Ghz RAM 256MB (DDR 2)	Comercial	X		
11	Cl (HANEL)		X		M. Board Intel d 201 GL8, Procesador Intel Celeron 1.33Ghz, RAM 256MB (DDR 2)	Comercial	X		
12	Cl (HANEL)		X		M. Board Intel d 201 GL8, Procesador Intel Celeron 1.33Ghz, RAM 256MB (DDR 2)	Comercial	X		
13	HANEL		X		M. Board Intel d101 GGE , Procesador Intel Celeron 2.66Ghz, RAM 256MB (DDR1)	Comercial	X		
14	AOPEN		X		M. Board Intel, Procesador Intel Celeron 1.86Ghz RAM 256MB (DDR1)	Recursos humanos	X		
15	Cl (HANEL)		X		M. Board Intel d 201 GL8, Procesador Intel Celeron 1.33Ghz, RAM 256MB (DDR 2)	Recursos humanos	X		
16	HANEL		X		M. Board Intel d101 GGE, Procesador Intel Celeron 600 Mhz, RAM 256MB (DIMM)	Economía	X		
17	HANEL		X		M. Board Intel d101 GGE, Procesador Intel Celeron 2.66Ghz, RAM 256MB (DDR1)	Economía	X		
18	Cl (HANEL)		X		M. Board Intel d 201 GL8, Procesador Intel Celeron 1.33Ghz, RAM 256MB (DDR 2)	Economía	X		
19	G-MAX		X		M. Board PSLk-CM, Procesador Pentium D 3.00Ghz RAM 1 GB(DDR2)	Economía	X		
20	AOPEN		X		M. Board AOPEN, Procesador Intel Celeron 2.66Ghz RAM 256MB (DDR1)	Economía	X		
21	AOPEN		X		M. Board Mx3W-Pro, Procesador Celaron 400 Mhz RAM 128 MB(DIMM	Economía	X		
22	LTEL		X		M. Board P5 VD2-Vm, Procesador Celeron D-3.06 Ghz RAM 256MB (DDR 2)	Servidor	X		
23	HANEL		X		M. Board Intel d101 GGE, Procesador Intel Celeron 2.66Ghz, RAM 256MB (DDR1)	Servidor	X		
24	Cl (HANEL)		X		M. Board Intel d 201 GL8, Procesador Intel Celeron 1.33Ghz, RAM 256MB (DDR 2)	Servidor	X		
25	VERSAT	X			Sistema contable certificado	Economía	X		

26	RH EXPERT	X			Sistema que trabaja con el expediente laboral de cada trabajador	Recursos humanos	X		
27	ENERGEST	X			Sistema que controla el combustible	Logística		X	
28	RED		X		Su uso permite la conexión con la intranet del MINAZ y de todas las demás UEB TECNOAZUCAR del país	Entidad	X		
29	Administra-dor de red			X	Se encarga del funcionamiento de los servidores, así como de la seguridad de la red y los equipos	Entidad		X	
30	Resp de seguridad informática			X	Encargado de velar por el cumplimiento del PSI y de la seguridad de los equipos.	Entidad		X	

Anexo 3 b) Clasificación de los recursos en la empresa ATI

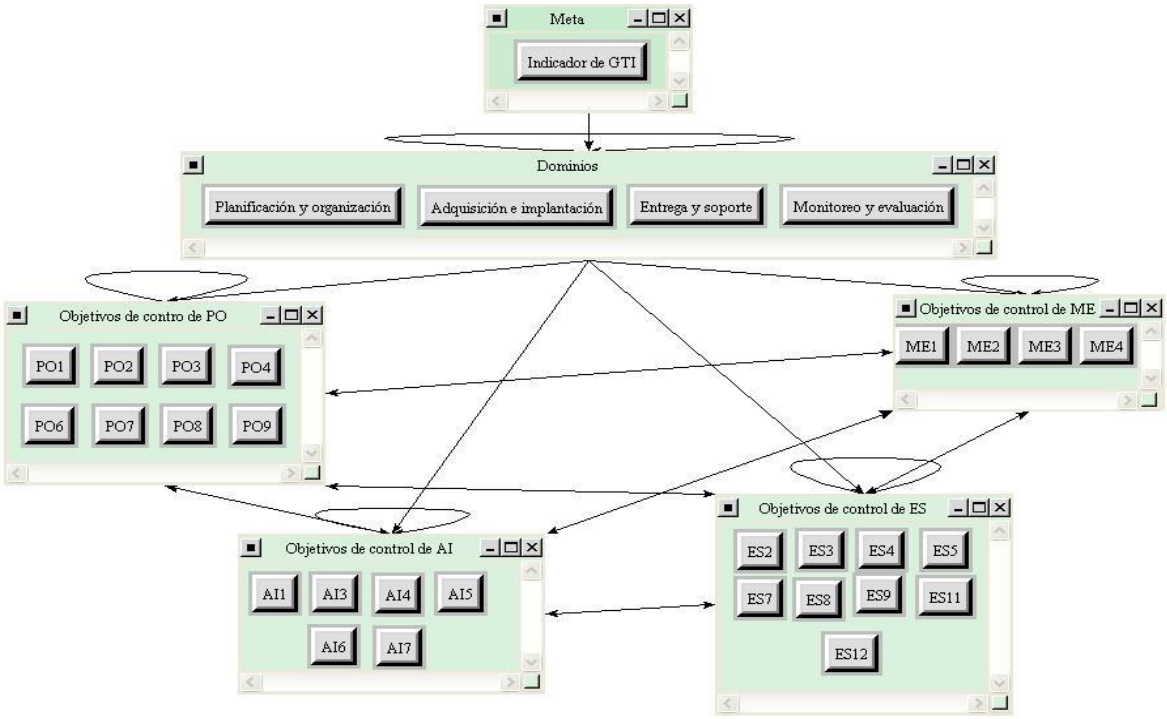
No	RECUR-SOS	CLASIFI-CACIÓN			ATI DESCRIPCION	PROCESO	IMPACTO		
		A	I	P			F	M	D
1	PC		X		Procesador Celeron, Frecuencia 600MHz RAM 128 MB, HD 60 GB	Abastec.		X	
2	PC		X		Procesador Celeron, Frecuencia 2,4 GHz RAM 256 MB, HD 80+80GB	Automática		X	
3	Toshiba		X		Procesador Celeron, Frecuencia 1,4GHz RAM 448 MB, HD 40 GB	Automática		X	
4	Fujitsu		X		Procesador Centrino Duo, Frecuencia 1,8GHz x 2 RAM 1 GB,HD 160 GB	Automática		X	
5	Fujitsu		X		Procesador Centrino Duo, Frecuencia 2,1GHz x 2 RAM 3 GB, HD 300 GB	Automática		X	
6	Fujitsu		X		Procesador Centrino Duo, Frecuencia 1,8GHz x 2 RAM 1 GB, HD 160 GB	Automática		X	
7	Toshiba		X		Procesador Pentium IV, Frecuencia 2,8 GHz RAM 512 MB, HD 80 GB	Automática		X	
8	PC		X		Procesador Celeron, Frecuencia 2,66GHz RAM 1 GB, HD 150 GB	Automática		X	
9	PC		X		Procesador Core 2, Frecuencia 2 x 1,8GHzRAM 1 GB, HD 150 GB	Calidad	X		
10	HP		X		Procesador Pentium M, Frecuencia 1,8 GHz RAM 512 MB, HD 80 GB	Dirección	X		
11	PC		X		Procesador Pentium II, Frecuencia 550MHz RAM 64 MB, HD 8 GB	Dirección			X
12	HP		X		Procesador Celaron M, Frecuencia 1,73 GHz RAM 1 GB, HD 80 GB	Economía	X		
13	PC		X		Procesador Core 2, Frecuencia 1,86 GHz RAM 1 GB, HD 160 GB	Economía	X		
14	PC		X		Procesador Core 2, Frecuencia 1,86 GHz RAM 1 GB, HD 160 GB	Economía	X		
15	PC		X		Procesador Pentium III, Frecuencia 1.0 GHz RAM 128 MB, HD 80 GB	Economía	X		
16	PC		X		Procesador Pentium III, Frecuencia 733 MHz RAM 256 MB, HD 20 GB	Economía	X		
17	PC		X		Procesador Pentium IV, Frecuencia 3,4 GHz RAM 512 MB, HD 160 GB	Economía	X		
18	PC		X		Procesador GPentium IV, Frecuencia 3,4	Economía	X		

					GHz RAM 512 MB, HD 160 GB				
19	Toshiba		X		Procesador Celeron, Frecuencia 2,4GHz RAM 256 MB, HD 40 GB	Electrónica		X	
20	Toshiba		X		Procesador Pentium IV, Frecuencia 2,8 GHz RAM 512 MB	Electrónica		X	
21	PC		X		Procesador Celeron, Frecuencia 2,4 GHz RAM 256 MB, HD 80GB	Electrónica		X	
22	PC		X		Procesador Pentium III, Frecuencia 733 MHz RAM 128 MB, HD 40 GB	Electrónica		X	
23	Toshiba		X		Procesador Celeron, Frecuencia 2,4GHz RAM 256 MB, HD 40 GB	GTP		X	
24	PC		X		Procesador Celeron, Frecuencia 3,0 GHz RAM 224 MB	GTP		X	
25	PC		X		Procesador Celeron, Frecuencia 1,8 GHz RAM 512 MB, HD 80GB	GTP		X	
26	Fujitsu		X		Procesador Centrino Duo, Frecuencia 2,1GHz x 2 RAM 3 GB, HD 300 GB	Ing.eléctrica		X	
27	HP		X		Procesador Pentium M, Frecuencia 1,8 GHz RAM 512 MB, HD 80 GB	Ing.eléctria		X	
28	PC		X		Procesador Celeron, Frecuencia 600 MHz RAM 64 MB, HD 17 GB	Ing.eléctrica		X	
29	PC		X		Procesador Pentium IV, Frecuencia 2,7GHz RAM 256 MB, HD 80 GB	Ing.eléctrica		X	
30	HP		X		Procesador Pentium M, Frecuencia 1,8 GHz RAM 512 MB, HD 80 GB	Laboratorio		X	
31	PC		X		Procesador Celeron, Frecuencia 2,66GHz RAM 192 MB, HD 150 GB	Laboratorio		X	
32	PC		X		Procesador Celeron, Frecuencia 500MHz RAM 256MB, HD 40 GB	Laboratorio		X	
33	PC		X		Procesador Celeron, Frecuencia 2,66GHz RAM 192 MB, HD 150 GB	Laboratorio		X	
34	PC		X		Procesador Celeron, Frecuencia 466MHz RAM 128 MB, HD 2.4 GB	Laboratorio		X	
35	PC		X		Procesador Celeron, Frecuencia 2,66 GHzRAM 256 MB, HD 80 GB	Laboratorio		X	
36	Toshiba		X		Procesador Celeron, Frecuencia 2,4 GHz RAM 256 MB, HD 40 GB	M.eléctricas		X	
37	Toshiba		X		Procesador Pentium IV, Frecuencia 2,8 MHz RAM 512 MB, HD 80 GB	M.eléctricas		X	
38	PC		X		Procesador Celeron, Frecuencia 600MHz RAM 128 MB, HD 60 GB	M.eléctricas		X	
39	PC		X		Procesador Pentium, Frecuencia 100 MHz RAM 80 MB, HD 4,7 GB	M.eléctricas		X	
40	PC		X		Procesador Pentium II, Frecuencia 400MHz RAM 128 MB, HD 2,37GB	Neumatica		X	
41	PC		X		Procesador Pentium, Frecuencia 200MHz RAM 64 MB, HD 17 GB	Neumática		X	
42	PC		X		Procesador Pentium II , Frecuencia 200 MHz RAM 96 MB, HD 17GB	Neumática		X	

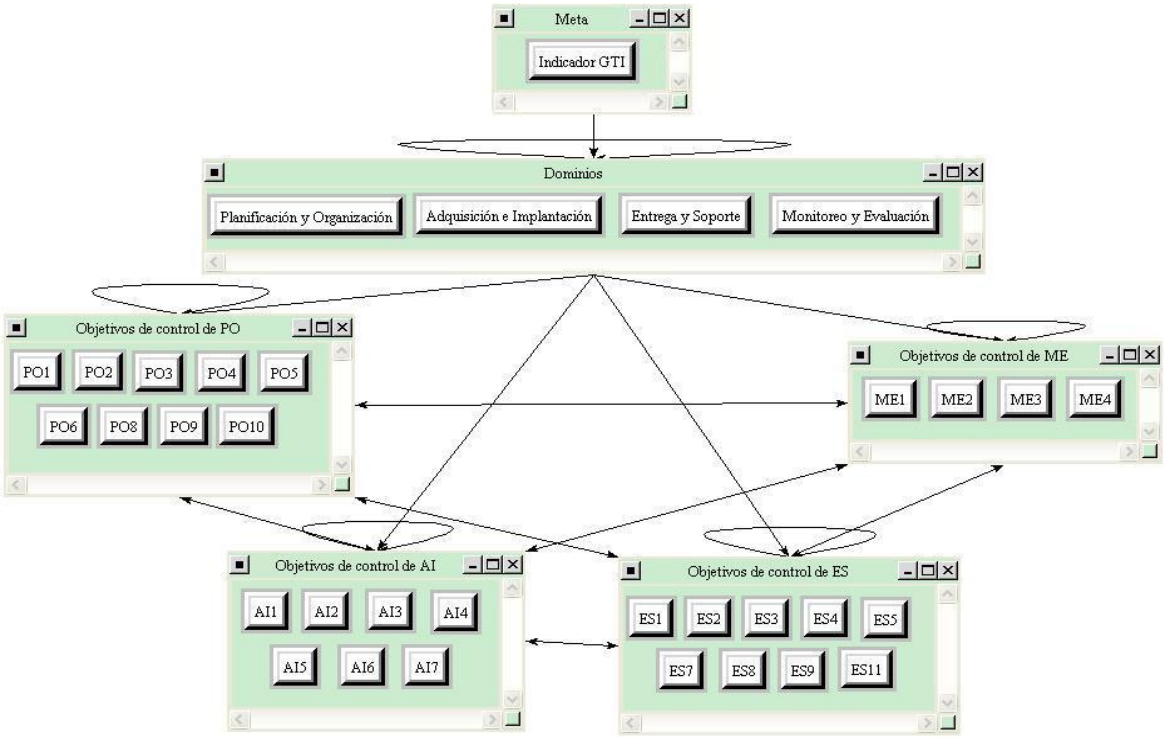
43	Fujitsu		X		Procesador Centrino Duo, Frecuencia 2,1GHz x 2 RAM 3 GB, HD 300 GB	Proyectos	X		
44	Fujitsu		X		Procesador Centrino Duo, Frecuencia 1,8GHz x 2 RAM 1 GB, HD 160 GB	Proyectos	X		
45	Fujitsu		X		Procesador Centrino Duo, Frecuencia 1,8GHz x 2 RAM 1 GB, HD 160 GB	Proyectos	X		
46	Fujitsu		X		Procesador Centrino Duo, Frecuencia 1,8MHz x 2 RAM 1GB, HD 80 GB	Proyectos	X		
47	Fujitsu		X		Procesador Pentium IV, Frecuencia 2GHz RAM 256 MB, HD 30 GB	Proyectos	X		
48	PC		X		Procesador Pentium III, Frecuencia 450MHz RAM 128 MB, HD 60 GB	Servidores	X		
49	PC		X		Procesador Pentium IV, Frecuencia 1,7GHz RAM 256 MB, HD 160 GB	Servidores	X		
50	HP-Proliant DL380G5		X		Procesador Xeon, Frecuencia 3,0 GHz RAM 4 GB, HD 4x146G	Servidores	X		
51	HP-Proliant ML350		X		Procesador Xeon, Frecuencia 3,2 GHz RAM 1 GB, HD 160 GB	Servidores	X		
52	Resp de seg informática			X	Encargado de velar por el cumplimiento del PSI de la entidad, así como de los recursos informáticos	Entidad		X	
53	Adminis-trador de red			X	Encargado de velar por el funcionamiento de la red interna de la entidad, así como de las conexiones dentro y fuera del país	Entidad		X	
55	ASSET PREMIUM	X			Control de la actividad económica	Grupo económico laboral	X		
56	CFT	X			Control de Producción	Grupo Técnico Productivo	X		
57	GTP	X			Control de Producción	Grupo técnico productivo	X		
58	RED		X			Entidad	X		

Categoría del riesgo	N	Vulnerabilidad	Amenaza	Descripción del Riesgo	Controles existentes	NP	MI	NR	Controles recomendados
SEGURIDAD	1	Falta de equipos para la sustitución en caso de roturas.	Pérdida de información valiosa o interrupción en la realización de cualquier proceso.	Si falla(n) algún(os) equipo(s) esto puede provocar retrasos en la entrega de información a las diferentes áreas y puede comprometer el cumplimiento de la misión en la entidad.	-Se realiza el mantenimiento y limpieza a los equipos semestralmente. -Cada trabajador es el encargado de velar por el funcionamiento de su equipo y reportar a su superior si éste presenta problemas.	A	B	B	Mantener los controles existentes.
	2	No se cuenta con sistema de alarma contra intrusos.	Pérdidas de equipos indispensables para la realización de la actividad laboral en la entidad, así como pérdidas de información.	La entrada no autoriza da de usuarios al centro puede comprometer la seguridad de la información, así como la de los propios equipos.	-En el horario de trabajo se ha dispuesto en la entrada del centro un puesto de recepción con un libro de visitas. -En el horario diurno está presente el trabajador de vigilancia. -Se tiene establecido el acceso a los locales donde exista TI.	B	M	B	-En cada local instalar rejas tanto en ventanas como en las puertas para así aumentar las medidas de seguridad. -Realizar mantenimiento de los llavines de los locales y verificar su funcionamiento.
	3	Cambio periódico de contraseñas	Accesos inapropiados	La ocurrencia de accesos inapropiados puede comprometer la confidencialidad e integridad de la información y el funcionamiento de los sistemas.	-En el plan seguridad informática están establecidas las medidas de cambio regular de contraseñas. -Cada máquina y usuario posee contraseña propia y se lleva a cabo el registro de uso.	A	A	A	Mantener un control periódico del estado de las instalaciones eléctricas.
DISPONIBILIDAD	4	No se cuenta con un sistema de aterramiento eléctrico.	-Pérdidas de equipos por alto voltaje o incendio en el sistema eléctrico. -Pérdida de información.	La falta de pararrayos puede ocasionar la pérdida de información así como de equipos de alto costo lo que compromete el funcionamiento de los procesos de la entidad.	-En caso de descargas eléctricas, el personal debe desconectar todo el equipamiento no imprescindible y en caso de ser severas desconectar los servidores y los módems.	M	A	M	Instalar un sistema de aterramiento y mantener los controles existentes.
	5	No todos los equipos cuentan con UPS	Fallas eléctricas	El no contar con todas las UPS necesarias puede ocasionar que las fallas eléctricas resulten en la pérdida de información.	No existen.	A	B	B	Valorar propuestas de inversión.
	6	No se cuenta con regulador	Pérdida de información por	El no contar con reguladores de voltaje repercute en la	Desconectar los equipos cuando ocurran problemas con el voltaje.	M	M	M	Valorar propuestas de inversión.

		de voltaje en los equipos.	pérdidas de equipos	realización de la actividad laboral y pérdida de tiempo importante.					
	7	Existencia de instalaciones eléctricas en los locales.	Incendio	Un incendio puede resultar en pérdidas costosas de activos de TI, de información de la entidad y de vidas humanas.	-Al final del pasillo de la empresa hay un extintor disponible. -Preservar todos los equipos posibles y las vidas humanas	A	A	A	Mantener un control periódico del estado de las instalaciones eléctricas.
	8	Existen 2 tipos de cuenta de correo electrónico (nacional e internacional).	Entradas de virus, pérdida de información.	Los ataques de virus pueden ocasionar la pérdida de la integridad de la información.	-Solo el director autoriza las cuentas de correo. -Se filtran los mensajes nacionales como internacionales para detectar cualquier anomalía. -Se mantiene un registro de correo internacional donde queda explícito quién envía, para quién va dirigido, motivo, país, fecha, hora.	B	B	B	Mantener los controles existentes.
	9	No se cuenta con sistema de alarma contra incendios y en los locales no hay presencia de extintores.	Pérdidas de vidas humanas, de equipos, y de información.	Repercute en el cumplimiento de la misión por parte de la organización y ocasiona grandes pérdidas.	Hay un balón y un área identificada para combatir los incendios.	A	A	A	Colocar extintores en cada área y realizar charlas acerca de cómo evitar y combatir la ocurrencia de incendios.
DESEMPEÑO	10	No se cuenta con planta eléctrica.	Pérdida de información, de tiempo importante para la realización de las actividades laborales.	Repercute en el compromiso de trabajo del hombre con la empresa.	El funcionamiento de la UEB respecto a sus actividades principales será en el edificio de la Delegación Provincial del MINAZ.	A	B	B	Valorar propuestas de inversión.

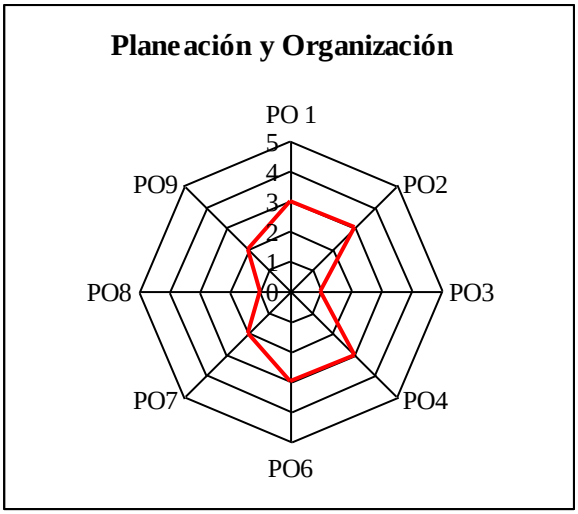


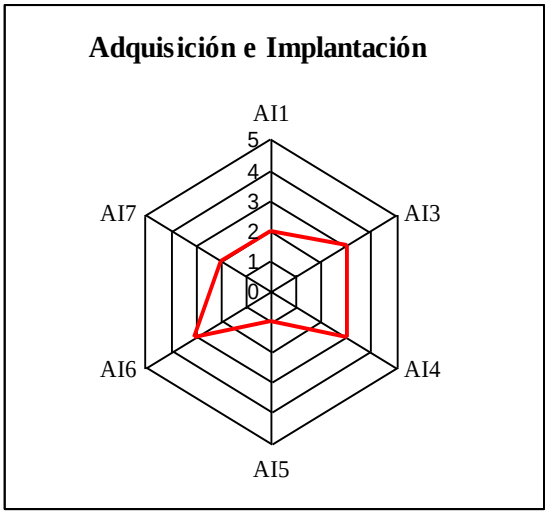
Anexo 5 a) Red del indicador de NGTI en la empresa TECNOAZUCAR

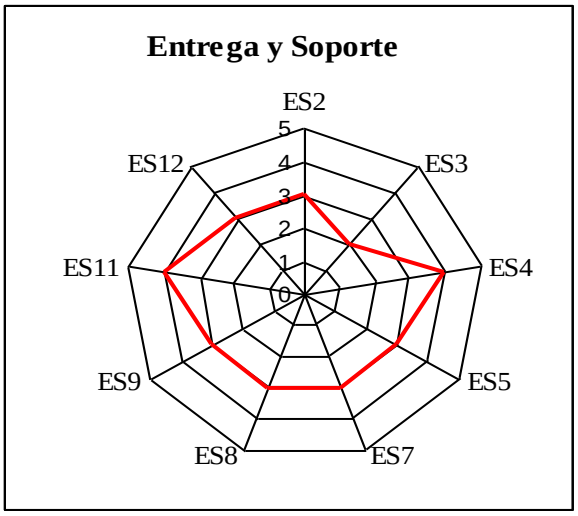


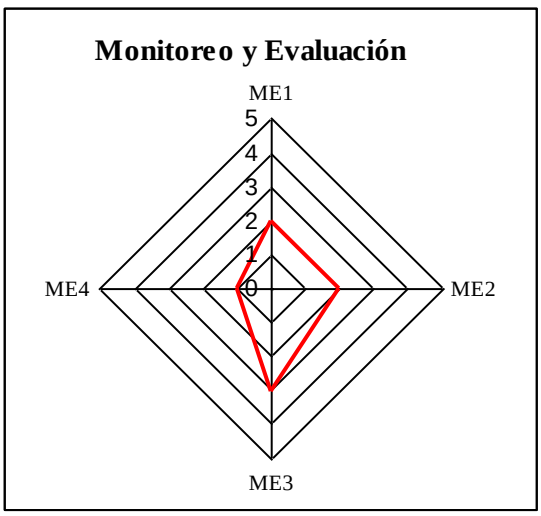
Anexo 5 b) Red del indicador de NGTI en la empresa ATI

Anexo 6 a) Radares de los dominios de TECNOAZUCAR









Anexo 6 b): Radares de los dominios de ATI