

**PROPUESTA DE MEJORAMIENTO Y CONTINGENCIA DE SISTEMAS
INFORMÁTICOS EN LA EMPRESA "T"**

ELABORADO POR
MARITZA YOHANA RAMÍREZ ROBAYO
EDWIN ALBERTO LONDOÑO RÚA
JAIRO ANDRÉS GÓMEZ GÓMEZ

UNIVERSIDAD EAN
FACULTAD DE POSTGRADOS
ESPECIALIZACIÓN GERENCIA INFORMÁTICA
BOGOTÁ
2012

**PROPUESTA DE MEJORAMIENTO Y CONTINGENCIA DE SISTEMAS
INFORMÁTICOS EN LA EMPRESA "T"**

ELABORADO POR
MARITZA YOHANA RAMÍREZ ROBAYO
EDWIN ALBERTO LONDOÑO RÚA
JAIRO ANDRÉS GÓMEZ GÓMEZ

TRABAJO DE GRADO IFI

DIRIGIDO POR
INGENIERO FREDY REYES

UNIVERSIDAD EAN
FACULTAD DE POSTGRADOS
ESPECIALIZACIÓN GERENCIA INFORMÁTICA
BOGOTÁ
2012

TABLA DE CONTENIDO

INTRODUCCIÓN	7
MARCO TEÓRICO	8
PROCESO DE CONSULTORÍA	8
¿Qué es una consultoría?	8
Rasgos particulares de la consultoría	9
Fases del proceso de consultoría	10
Tipos de consultores.....	21
Gestión del Conocimiento en Consultoría	22
EVALUACIÓN DE MODELOS DE MADUREZ INFORMÁTICA.....	26
El modelo de Nolan/Gibson	26
El modelo de Nolan	28
El modelo de Gartner.....	29
El modelo de Donovan	32
CMMI	34
PLAN DE CONTINGENCIA INFORMÁTICA.....	36
Definición.....	36
Consideraciones de implementación	38
Etapas para elaborar un Plan de Contingencia	39
Norma ISO 27001, Guía de buenas prácticas ISO 27002 y necesidad del Plan de Contingencia.....	43
MODELO DE GOBIERNO TI BASADO EN COBIT	48
ESTÁNDAR PARA LA GESTIÓN DE SERVICIOS INFORMÁTICOS ITIL	51
El ciclo de vida ITIL.....	52

CAPITULO 1	54
1. ANÁLISIS Y DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DEL DEPARTAMENTO DE SISTEMAS Y SU ROL EN LA ORGANIZACIÓN.	54
1.1. Evaluación de la madurez de TIC en la empresa “T”	54
1.1.1. Tecnologías	54
1.1.2. Motivaciones de la organización hacia la informática	58
1.1.3. Nivel de participación y asimilación de las TIC por los usuarios	59
1.1.4. Metodologías y procedimientos	60
1.1.5. Carácter de la gerencia informática	62
1.1.6. Conclusión final.....	63
1.2. Revisión de los procesos actuales del departamento de sistemas en la empresa “T”	66
1.2.1. Procesos de gestión de los sistemas de información	66
1.2.2. Procesos de gestión de infraestructura de TI	67
1.2.3. Procesos de planeación de TIC	68
1.2.4. Procesos de organización de TI.....	69
1.3. Evaluación del estado de tecnologías en la empresa “T”	69
1.3.1. Matriz de las 4 Acciones	72
1.3.2. Matriz DOFA (Debilidades – Oportunidades – Fortalezas – Amenazas)	73
1.3.3. Análisis y Priorización de Estrategias	76
1.4. Identificación de necesidades de TI en la empresa “T”	77
CAPITULO 2	81
2. IDENTIFICACIÓN DE PROCESOS Y METODOLOGÍAS DE TICS NECESARIOS PARA LA MEJORA	81
2.1. Practicas recomendadas para la mejora de los procesos actuales.....	81
2.1.1. Procesos de Gestión de los Sistemas de Información	81

2.1.2.	Procesos de Gestión de Infraestructura de TI	84
2.1.3.	Procesos de planeación de TI	88
2.1.4.	Procesos de organización de TI	90
3.	PLAN DE CONTINGENCIA DE TI PARA EL SISTEMA DE INFORMACIÓN CORPORATIVO	93
3.1.	Alcance	93
3.2.	Objetivo general	93
3.3.	Objetivos específicos	93
3.4.	Descripción del servicio	94
3.5.	Análisis y valoración de riesgos	97
CAPITULO 4.....		109
4.	PROPUESTA DE MEJORAMIENTO	109
4.1.	Servicio de mesa de ayuda	109
4.1.1.	Objetivos de la mesa de ayuda	109
4.1.2.	Componentes del servicio	109
4.1.3.	Estructura básica de la mesa de ayuda.....	111
4.1.4.	Responsables del servicio	111
4.1.5.	Matriz RACI	112
4.1.6.	Definición de los incidentes	113
4.1.7.	Acuerdos de nivel de operación (OLA's)	113
4.1.8.	Mapa del servicio mesa de ayuda	114
4.2.	Implementación de herramientas para gestión de TI	116
4.2.1.	Sistema Help Desk	116
4.2.2.	Inventarios de Hardware y Software.....	119
4.2.3.	Control remoto y soporte	120

4.3. Gestión administrativa.....	122
CONCLUSIONES	127
BIBLIOGRAFÍA	129
FICHA BIBLIOGRÁFICA DEL TRABAJO	130
ANEXO 1	133
Resultados de la encuesta a usuarios y líderes de área	133
Relación de la encuesta con la calificación de Madurez Informática	134
Desarrollo de la encuesta	135
ANEXO 2	150
Documento de requerimientos	150
ANEXO 3	152
Documento de planeación	152
ANEXO 4	154
Formato gestión de cambios.....	154
ANEXO 5	156
Documento de pruebas.....	156
ANEXO 6	158
Documento de capacitación.....	158
ANEXO 7	160
Acta de reunión.....	160
ANEXO 8	162
Adquisición de software	162

INTRODUCCIÓN

Todas las organizaciones, de cualquier tamaño, naturaleza, actividad económica, etc., son susceptibles de mejora en algunos de sus procesos de negocio o de apoyo. Conscientes de esto, tomamos la determinación de aprovechar nuestra experiencia y aplicar los conocimientos adquiridos durante la especialización para promover la mejora en el proceso de Tecnologías de Información y Comunicación (TIC) en una compañía de nuestro interés, que en adelante llamaremos “T”, a través de la metodología de la consultoría.

No se puede mejorar lo que no se conoce, por lo que el punto de partida definido fue realizar un acercamiento a la empresa “T”, conocer su proceso de TIC y comprender la visión del recurso humano del área de Sistemas sobre el estado informático de la organización. Posteriormente, se plantea la necesidad de evaluar la madurez informática de la compañía, para lo cual se analiza también la percepción del usuario final o cliente interno, buscando tener una idea objetiva y evitar opiniones sesgadas.

Con el análisis de la información recolectada, el equipo consultor y el grupo de trabajo de Sistemas de la compañía detectan las problemáticas de TI y generan las estrategias orientadas a promover la mejora del área y de los servicios informáticos para beneficio de la organización.

El equipo consultor sugiere también una propuesta de mejoramiento, basada en guías de buenas prácticas de TI y en su propia experiencia.

Este documento presenta el desarrollo del mencionado proceso de consultoría y los resultados obtenidos representados en una propuesta de mejoramiento y un plan de contingencia de TI.

MARCO TEÓRICO

PROCESO DE CONSULTORÍA

¿Qué es una consultoría?

La consultoría es un servicio profesional prestado a una empresa, con el fin de identificar, definir, solucionar problemas existentes que la afectan; con esto se busca cumplir las metas, objetivos y propósitos trazados por la empresa.¹

La consultoría no cuenta con procedimiento estándar y se realiza de diferentes maneras debido que cada empresa cuenta con su propia personalidad, objetivos y maneras de desempeñarse. Por lo tanto, se debe realizar un análisis profundo de los hechos, generando soluciones factibles y realizables según los objetivos planteados en cada empresa.

Por lo tanto la consultoría es una labor en la cual se proporciona ayuda a una situación que altere el normal desarrollo de la empresa. La consultoría debe ser realizada por una persona especializada en el campo que se está evaluando y asesorando. Es un proceso en el que la teoría y la practica se combinan adecuadamente; su resultado no puedes ser producto de la inspiración, debe ser producto de un exhaustivo análisis de todas las variables que intervienen en el proceso.

Por último la consultoría debe contar con agentes externos con el fin de tener una visión de imparcialidad, con el fin de hallar un resultado final sincero y obtener

¹ Centro integral de asesoría y consultoría – CIAC. ¿Qué es una consultoría?.

<http://www.udem.edu.co/UDEM/Extension/CentroAsesoriasConsultorias/infoInteres.htm>

recomendaciones francas para que la empresa pueda mejorar y así evitar que el proceso sea viciado con ninguna asociación directa de la empresa.

Rasgos particulares de la consultoría²

- La consultoría es un servicio independiente:

Se caracteriza por la imparcialidad del consultor, que es un rasgo fundamental de su papel, lo cual significa al mismo tiempo una relación muy compleja con las organizaciones clientes y con las personas que trabajan en ellas.

- La consultoría es esencialmente un servicio consultivo:

No se contrata a los consultores para dirigir organizaciones o para tomar decisiones en nombre de directores en problemas. Su papel es actuar como asesores, con responsabilidad por la calidad e integridad de su consejo; los clientes asumen las responsabilidades que resulten de la aceptación de dicho consejo. No solo se trata de dar el consejo adecuado, sino de hacerlo de manera adecuada y en el momento apropiado.

- La consultoría es un servicio que proporciona conocimientos y capacidades profesionales para resolver problemas prácticos:

Una persona llega a ser consultor de empresas en el pleno sentido del término después de haber acumulado una masa considerable de conocimientos sobre los diversos problemas y situaciones que afectan a las empresas y adquirido la capacidad necesaria para identificarlos, hallar la información pertinente, analizar y sintetizar, elegir entre posibles soluciones, comunicarse con personas, etc.

² Manual de Formación de Consultoría. Ing. Francisco Meza. Ing. Miguel Obregón. IBM Educación; Junio, 1997

Parte de este conocimiento se debe transferir a la organización durante el servicio de consultoría, de modo que aquella logre desarrollar capacidad propia para resolver sus problemas.

- La consultoría no proporciona soluciones milagrosas.

Sería un error suponer que, una vez contratado el consultor, las dificultades desaparecen. La consultoría es un trabajo difícil basado en el análisis de hechos concretos y en la búsqueda de soluciones originales pero factibles.

Fases del proceso de consultoría^{3 4}

El proceso de consultoría comprende las siguientes etapas:

Iniciación

En esta fase el consultor comienza a trabajar con un cliente. Esta fase incluye sus primeros contactos, las conversaciones acerca de lo que el cliente desearía modificar en su organización y de qué manera el consultor podría prestarle ayuda, la aclaración de sus papeles respectivos, la preparación de un plan de tareas basado en un análisis preliminar del problema y la negociación y concertación de un contrato de consultoría. Se trata de una fase preparatoria y de planificación. No obstante, a menudo se insiste en que esta fase establece los cimientos para todo lo que seguirá, dado que las fases siguientes estarán fuertemente influidas por la calidad del trabajo conceptual realizado y por el tipo de relaciones que el consultor establezca con su cliente desde el comienzo.

³ Marisol Pérez Campaña, Luis Álvarez López, Enrique Zayas Miranda. Consultoría Organizacional. <http://www.monografias.com/trabajos15/consultoria-organizacional/consultoria-organizacional.shtml>

⁴ Luís Alvarez. Proceso de consultoría organizacional. <http://www.gestiopolis.com/recursos4/docs/ger/econsultoria.htm>

En esta fase inicial puede asimismo suceder que una propuesta de cometido no se prepare a satisfacción del cliente, o que se pida a varios consultores que presenten propuestas, entre las que se elegirá una para realizar la tarea.

La etapa de preparación inicial, iniciación o entrada debe permitir al cliente y los consultantes un aprendizaje mutuo, es una fase de adaptación, pero en ella también se inicia la exploración de la organización cliente y se formulará el plan a seguir en la intervención.

Es recomendable iniciar el trabajo de Información/Formación por contactos iniciales con el máximo líder de la organización y colaboradores cercanos donde se formalicen cuestiones de amplio interés para el trabajo, se investiguen las expectativas y se aclaren los roles cuidando que en todo momento quede claro que la labor de los consultores es de asesoría, capacitación y ayuda en transferencia tecnológica, etc. y nunca tendrá autoridad para tomar decisiones del qué hacer y otras que son responsabilidad de los directivos.

El intercambio con los consejos de dirección o juntas directivas posibilitará ambas tareas y permitirá ir realizando un diagnóstico inicial que después el equipo complementará.

Es importante en este inicio preparar a los trabajadores y directivos en la solución de problemas e ir introduciéndolos en el uso de técnicas que serán de utilidad en todo el trabajo, especial dedicación debe hacerse a la preparación de los consultores internos que serán la semilla de la mejora continua y los líderes de esta en la organización.

En resumen lo que se debe lograr en esta etapa:

- Intercambio de expectativas de metas, roles y responsabilidades.

- Acuerdo sobre términos, métodos y técnicas a utilizar.
- Preparación inicial de todos los implicados y en especial los equipos de consultores internos.
- Acciones de arriba – abajo empezando por la alta dirección (talleres, sesiones de trabajo).
- Realización de un diagnóstico preliminar en conjunto por los consultores internos y externos.
- Elaboración de la planificación de la tarea a realizar, discusión y aprobación de la propuesta.

Diagnóstico

La segunda fase es un diagnóstico a fondo del problema que se ha de solucionar, basado en una investigación cabal de los hechos y en su análisis. Durante esta fase, el consultor y el cliente cooperan para determinar el tipo de cambio que se necesita. ¿Es el problema fundamental del cambio de índole tecnológica, organizativa, de información, psicológica o de otro tipo? Si tiene todas estas dimensiones ¿Cuál es el esencial? ¿Qué actitudes imperan en la organización con respecto al cambio? ¿Se comprende la necesidad del cambio o será preciso persuadir a los miembros de la organización de que tienen que cambiar? Se utilizan los resultados de la fase de diagnóstico y se extraen conclusiones sobre cómo orientar el trabajo con respecto a las necesidades propuestas con el fin de que se resuelva el problema real y se obtengan los beneficios deseados. Durante esta fase se pueden vislumbrar algunas posibles soluciones.

La investigación y el diagnóstico de los hechos reciben a menudo escasa atención. Sin embargo, las decisiones con respecto a saber qué tipo de datos se han de buscar, qué datos se han de omitir, qué aspectos del problema conviene examinar a fondo y qué hechos se pueden dejar a un lado predeterminan la pertinencia y la calidad de las soluciones que se propondrán. Por otra parte, con la recolección de los datos el consultor ya está influyendo en el sistema del cliente, y los miembros de la organización tendrán que empezar ya a cambiar como resultado de la presencia del consultor.

El objetivo del diagnóstico es definir los problemas que afronta el cliente, examinar de forma detallada sus causas y preparar toda la información necesaria para orientar las decisiones que han de ser tomadas para la solución. En principio el diagnóstico no incluye la actividad destinada a resolver los problemas, esta se llevará a cabo en la fase siguiente, e incluso puede que el propio diagnóstico lleve a la conclusión que algún problema no puede ser resuelto o no valga la pena hacerlo por diversas razones reales e incluso infundadas o de poco peso. Sin embargo, en la práctica es muy difícil establecer una línea estricta divisoria entre diagnóstico y planeación de acción. Con frecuencia ocurre que en el diagnóstico se vayan determinando y estudiando posibles variantes de solución.

Plan de Acción

La tercera fase tiene por objetivo hallar la solución del problema. Abarca el estudio de las diversas soluciones, la evaluación de las opciones, la elaboración de un plan para introducir los cambios y la presentación de propuesta al cliente para que éste adopte una decisión. El consultor puede optar entre una amplia gama de técnicas, en particular si la participación del cliente en esta fase es activa. La planificación de la acción requiere imaginación y creatividad, así como un enfoque riguroso y sistemático para determinar y estudiar las opciones posibles, eliminar propuestas que podrían conducir a cambios de escasa importancia e innecesarios y decidir qué solución se ha de adoptar. Un aspecto importante del plan de acción consiste en elaborar una estrategia y tácticas

para la introducción de los cambios, en particular para abordar los problemas humanos que se pueden prever y para superar cualquier resistencia al cambio. Las soluciones o acciones que se proyecten en sentido general pueden ser clasificadas de manera general en dos grupos.

1. Acciones directas.

2. Acciones indirectas

Las acciones directas por lo general tienen las siguientes características.

- Dependen de una decisión interna, siendo por lo general su origen derivado de factores objetivos que en su mayoría tienen un consenso aplastante.
- Van dirigidas a una o pocas dimensiones esenciales muy concretas.
- Son por lo general correctivo o de generalización, no requiriendo estudios adicionales muy profundos y/o complejos, estando en su mayoría estructuradas.
- Por regla general sus resultados son palpables de inmediato o en cortos plazos.
- No representan grandes inversiones de recursos humanos, materiales y/o financieros.

Las acciones clasificadas como indirectas por lo general tienen las siguientes características:

- Dependen de una decisión externa, la acción en si consiste en convencer, fundamentar la necesidad, buscar apoyo, aprobación en las instancias superiores.

- Dependen de una decisión interna pero las acciones definitivas surgirán después de un estudio más profundo, el cual por lo general es complejo y no tiene soluciones estructuradas.
- Requieren de una preparación previa requiriendo ésta plazos normalmente medios o largos, la acción en sí es la preparación de dichas condiciones, las cuales no pocas veces demandan esfuerzos multidisciplinarios.

Aplicación, implementación o puesta en práctica

La puesta en práctica, que es la cuarta fase de la consultoría, constituye una prueba definitiva con respecto a la pertinencia y viabilidad de las propuestas elaboradas por el consultor en colaboración con su cliente. Los cambios propuestos comienzan a convertirse en una realidad. Empiezan a suceder cosas, que se han planificado o que escapan a la planificación. Pueden surgir nuevos problemas y obstáculos imprevistos o se puede poner de manifiesto el carácter erróneo de ciertas suposiciones o errores de planificación, la resistencia al cambio puede ser muy distinta de la que se preveía en la fase de diagnóstico y planificación. Quizás sea necesario corregir el diseño original y el plan de acción. Como es imposible prever con exactitud todas las relaciones, acontecimientos o actitudes, y la realidad de la puesta en práctica difiere a menudo del plan, la vigilancia y administración de la aplicación son muy importantes. Esto explica también por qué prefieren los consultores profesionales participar en la puesta en práctica de los cambios que han contribuido a identificar y planificar.

Una vez que el equipo de diseño elaboró el plan de acción y este fue sometido a la consideración de la alta dirección de la organización y aprobado, se inicia la etapa de implementación. La implementación tiene como objetivo implantar las acciones derivadas de la estrategia de solución.

Las tareas o actividades a desarrollar en esta etapa son las siguientes:

- Preparar las condiciones para la implementación.
- Implementación de cada acción.

La etapa de implementación en general es una etapa de ejecución donde los implicados y responsables deben asegurarse que las acciones previstas se lleven a cabo según lo aprobado de la manera más rigurosa posible.

En primer lugar resulta necesario preparar las condiciones requeridas para implementar cada acción acorde a los plazos establecidos; dependiendo del tipo de acción la tarea tendrá diferentes matices.

La creación de condiciones para dejar implantadas acciones clasificadas como directas consiste en esencia en garantizar los recursos necesarios y la preparación del personal para su puesta en práctica y una vez que esto este concluido implementarla.

En el caso de las acciones de tipo indirecto la situación es un poco más compleja ya que prácticamente puede llevar al equipo que las ejecuta a iniciar un proceso investigativo específico con procedimientos particulares para poder llegar a precisar acciones directas, o sea, que prácticamente implica todo un trabajo de diseño, Informativo, formativo y comprometedor alto que tiene que ser tomado muy en cuenta si se quiere alcanzar el éxito en la misma. Por lo regular, deben implementarse acciones de formación para los directivos y el staff donde cada cual adquiera los conocimientos y desarrolle las habilidades para utilizarlo tal y como fue concebido.

En la etapa de implementación pueden y de hecho deben ser aplicadas diversas técnicas teniendo primacía las que ayuden a planificar y controlar los avances, tal es el caso de los diagramas de Gant, los de secuencia o flujo de actividades y documentos, así como técnicas de apoyo a la exposición de ideas para ser usadas en la formación. El equipo de implementación debe además asegurar que se elabore y este a

disposición de los trabajadores y directivos toda la documentación requerida, en términos de normas, procedimientos, etc. Por último son muy importantes las acciones de seguimiento necesarias para valorar los avances operados en la ejecución e ir corrigiendo las posibles desviaciones existentes.

Terminación, evaluación y ajustes

La quinta y última fase en el proceso de consultoría incluye varias actividades. El desempeño del consultor durante su cometido, el enfoque adoptado, los cambios introducidos y los resultados logrados tendrán que ser evaluados por el cliente y por la organización de consultoría. Se presentan y aprueban los informes finales. Se establecen los compromisos mutuos. Si existe interés en continuar la relación de colaboración, se puede negociar un acuerdo sobre el seguimiento y los contactos futuros. Una vez completadas estas actividades, el consultor se retira de la empresa del cliente y la tarea o el proyecto de consultoría queda terminado de común acuerdo.

La etapa también conocida como de evaluación y ajustes como última etapa de ciclo de mejora continua tiene a la vez la característica de ser prácticamente la que abre un nuevo ciclo. El objetivo de esta etapa es evaluar, sí con la aplicación del plan de acción se alcanzan los resultados esperados en términos de objetivos organizacionales, personales y sociales, así como realizar los ajustes, necesarios del plan de acción.

La etapa de evaluación y ajustes en su contenido contendrá por tanto los aspectos fundamentales de las etapas anteriores y ella es la que mantendrá abierto eternamente el ciclo de mejora continua. Como las acciones específicas son diversas y generan expectativas de resultados en plazos de tiempo diferentes, deberán evaluarse sistemáticamente los resultados a partir de la información existente que normalmente es recopilada, esto permitirá a la alta dirección tener la retroalimentación básica necesaria.

Los consultores externos podrán participar si así se dispone y acuerda en el seguimiento, pero pueden perfectamente no hacerlo y esta tarea de seguir en el proceso de mejora continua quedar en manos de los directivos, trabajadores y consultores internos de la Organización.

Tabla 1. Esquema General de las Fases y procesos en Consultoría.

Fases	Procesos		
	Contenido	Operativo	Gerencial
<p>1. Iniciación (Preparación inicial)</p> <ul style="list-style-type: none"> • Primeros contactos con cliente • Diagnostico preliminar • Planear el cometido • Propuesta de tareas • Contrato 	<ul style="list-style-type: none"> • Calificar el contenido • Situar el contexto 	<ul style="list-style-type: none"> • Entrevistas preliminares • Elaboración proposición preliminar 	<ul style="list-style-type: none"> • Pide la intervención • Intenciones reales
<p>2. Diagnóstico</p> <ul style="list-style-type: none"> • Descubrir los hechos • Análisis y síntesis • Examen detallado del problema 	<ul style="list-style-type: none"> • Analizar el sistema del cliente • Identificar problemas • Encontrar un modelo explicativo 	<ul style="list-style-type: none"> • Análisis documental. • Entrevistas • Análisis de flujo 	<ul style="list-style-type: none"> • Comunicación • Confianza • Apertura Vs. Resistencia
<p>3. Planificación de medidas (Plan de acción)</p> <ul style="list-style-type: none"> • Elaborar soluciones • Evaluar opciones • Propuesta al cliente • Planear la aplicación de medidas 	<ul style="list-style-type: none"> • Busca de alternativas • Elección del modelo explicativo • Prueba “piloto” de soluciones 	<ul style="list-style-type: none"> • Elaboración de documento con propuestas 	<ul style="list-style-type: none"> • Poder del consultor en la toma de decisiones • Integrador de grupos

<p>4. Aplicación (Implementación)</p> <ul style="list-style-type: none"> • Contribuir a la aplicación • Propuesta de ajustes • Capacitación 	<ul style="list-style-type: none"> • Presentación interactiva de las soluciones • Ajuste de situaciones específicas • Participar (o no) en la implementación. • Retroalimentación. 	<ul style="list-style-type: none"> • Participación en la solución • Ajustes 	<ul style="list-style-type: none"> • Reacciones de la empresa • Logros obtenidos Vs. resultados esperados.
<p>5. Terminación</p> <ul style="list-style-type: none"> • Evaluación • Informe final • Establecer compromisos • Planes de seguimiento • Retirada 	<ul style="list-style-type: none"> • Evaluación 	<ul style="list-style-type: none"> • Evaluación 	<ul style="list-style-type: none"> • Evaluación

Fuente: MsC Luís F Alvarez López - Estrategia y dirección estratégica. ⁵

⁵ Luís Alvarez. Proceso de consultoría organizacional. <http://www.gestiopolis.com/recursos4/docs/ger/econsultoria.htm>

Tipos de consultores

Los servicios de consultoría pueden ser desarrollados por dos tipos de consultores, personal externo a la organización, que es el caso más generalizado cuando se desea aplicar enfoques o técnicas sobre los cuales la organización no cuenta con especialistas; o también puede ser desarrollado por personal interno, cuando se utilizan directivos o especialistas de la propia organización. A continuación se mencionan las ventajas y desventajas según el tipo de consultor.

Tabla 2. Tipos de Consultores. Autor: Alexis Codina⁶.

	Ventajas	Desventajas
Consultores Externos	<ul style="list-style-type: none"> • Es un “extraño”, “independiente”. • Juicio “fresco”, imparcial y no comprometido con los problemas de la organización. • Puede transmitir experiencias de otras organizaciones • Maneja enfoques, técnicas y experiencias sobre procesos de consultoría. • Mayor credibilidad que otros miembros de la empresa. 	<ul style="list-style-type: none"> • No conoce la estructura, la cultura organizacional, ni las personas. • Debe emplear algún tiempo en “familiarizarse”. • Nunca conocerá la organización como los que “viven” en ella.
Consultores Internos	<ul style="list-style-type: none"> • Conoce profundamente la estructura, las personas y los procedimientos de la organización. 	<ul style="list-style-type: none"> • Se le considera “de la familia”. • Puede influenciarse por prejuicios o por la “historia”. • Depende de la organización.

⁶ Alexis Codina. La consultoría: difusión de tecnología y formación gerencial.
http://www.degerencia.com/articulo/la_consultoria_difusion_de_tecnologia_y_formacion_gerencial

	<ul style="list-style-type: none"> • Está “disponible” dentro de la organización en todo momento. • Es un especialista en algún área o proceso de la empresa. • Conoce los problemas de la empresa a fondo. 	<ul style="list-style-type: none"> • No puede aportar experiencias de otros sitios. • Puede tener menos credibilidad y autoridad que un externo.
--	--	--

Fuente: degerencia.com⁷

Gestión del Conocimiento en Consultoría⁸

La Gestión del Conocimiento es, en definitiva, la gestión de los activos intangibles que generan valor para la organización. La mayoría de estos intangibles tienen que ver con procesos relacionados de una u otra forma con la captación, estructuración y transmisión de conocimiento. Por lo tanto, la Gestión del Conocimiento tiene en el aprendizaje organizacional su principal herramienta. La Gestión del Conocimiento es un concepto dinámico o de flujo, según sea definida la estrategia de implantación y uso.

Para un mejor entendimiento se debe establecer cuál es la diferencia entre dato, información y conocimiento. Una primera aproximación podría ser la siguiente: los datos están localizados en el mundo y el conocimiento está localizado en agentes (personas, organizaciones,...), mientras que la información adopta un papel mediador entre ambos conceptos.

Hay que reconocer que, en realidad, lo que fluye entre agentes distintos nunca es conocimiento como tal, sino datos (información). Es posible aproximar el conocimiento

⁷ Alexis Codina. La consultoría.

http://www.degerencia.com/articulo/la_consultoria_difusion_de_tecnologia_y_formacion_gerencial

⁸ Fundación IberoAmericana del Conocimiento. Gestión del Conocimiento en Consultoría. <http://www.gestiondelconocimiento.com/introduccion.htm>

de dos agentes que comparten los mismos datos, pero debido a sus experiencias anteriores y a las diferencias en el modo de procesar los datos (modelos mentales, modelos organizacionales), nunca tendrán las mismas tendencias para la acción, ni estados idénticos de conocimiento. Sólo podemos conseguir aproximaciones, ya que el contexto interno y externo de un agente siempre es diferente a otro. Esto es así, porque el conocimiento es información puesta dentro de un contexto (experiencia).

En definitiva, los datos, una vez asociados a un objeto y estructurados se convierten en información. La información asociada a un contexto y a una experiencia se convierte en conocimiento. El conocimiento asociado a una persona y a una serie de habilidades personales se convierte en sabiduría, y finalmente el conocimiento asociado a una organización y a una serie de capacidades organizativas se convierte en Capital Intelectual.

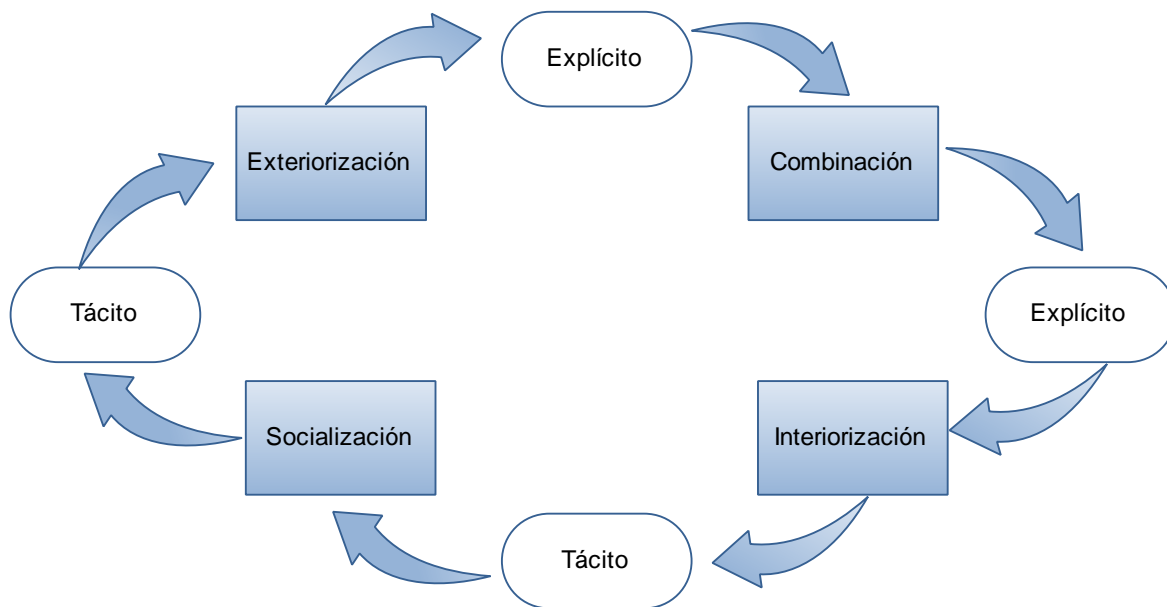
Proceso de Creación del Conocimiento⁹

El proceso de creación del conocimiento para Nonaka y Takeuchi (1995) es a través de un modelo de generación de conocimiento mediante dos espirales de contenido epistemológico y ontológico.

Es un proceso de interacción entre conocimiento tácito y explícito que tiene naturaleza dinámica y continua. Se constituye en una espiral permanente de transformación interna de conocimiento, desarrollada siguiendo 4 fases como se muestra de forma gráfica en la siguiente figura:

⁹ Fundación IberoAmericana del Conocimiento. Modelo nonaka.
http://www.gestiondelconocimiento.com/modelo_nonaka.htm

Figura 1: Procesos de conversión del conocimiento en la organización.



Fuente: Nonaka y Takeuchi, 1995.

- La Socialización, es el proceso de adquirir conocimiento tácito a través de compartir experiencias por medio de exposiciones orales, documentos, manuales y tradiciones y que añade el conocimiento novedoso a la base colectiva que posee la organización.
- La Exteriorización, es el proceso de convertir conocimiento tácito en conceptos explícitos que supone hacer tangible mediante el uso de metáforas conocimiento de por sí difícil de comunicar, integrándolo en la cultura de la organización; es la actividad esencial en la creación del conocimiento;
- La combinación, es el proceso de crear conocimiento explícito al reunir conocimiento explícito proveniente de cierto número de fuentes, mediante el intercambio de conversaciones telefónicas, reuniones, correos, etc., y se puede

categorizar, confrontar y clasificar para formar bases de datos para producir conocimiento explícito.

- La Interiorización, es un proceso de incorporación de conocimiento explícito en conocimiento tácito, que analiza las experiencias adquiridas en la puesta en práctica de los nuevos conocimientos y que se incorpora en las bases de conocimiento tácito de los miembros de la organización en la forma de modelos mentales compartidos o prácticas de trabajo.

Para Nonaka y Takeuchi, lo expresado por Peter Drucker en el sentido que, la esencia de la dirección es, cómo se puede aplicar de la mejor forma un conocimiento existente para poder crear otro conocimiento nuevo o reciclado, es justificado ya que sus estudios en compañías japonesas respaldan el proceso de creación del conocimiento que ambos japoneses han sostenido.

Proceso de Creación del Conocimiento

Teniendo en cuenta lo mencionado, se identifica la importancia de que la organización adopte los conocimientos generados durante el proceso de consultoría. Para lograr este cometido, es definida una metodología de primera fase para la gestión del conocimiento, en la cual se comparten experiencias mediante la interacción entre consultores y colaboradores de la organización, además de documentar las experiencias y conocimientos para que sean posteriormente usados con un alto grado de autonomía.

El proceso de gestión del conocimiento es un proceso continuo que se lleva a cabo durante toda la ejecución de la consultoría. En las fases de la consultoría de APLICACIÓN y TERMINACIÓN se evidencia que se llevan a cabo procesos documentales formales de conocimiento, compromisos y evaluación que miden el desempeño del proyecto y se establecen en ellos unos lineamientos de conocimiento.

EVALUACIÓN DE MODELOS DE MADUREZ INFORMÁTICA

Desde el momento en que Richard Nolan introdujo en 1973 su "modelo por etapas" para la aplicación de TI en organizaciones, son muchos los que han propuesto modelos de mejora gradual. Estos modelos se convirtieron en instrumentos adecuados para desarrollar programas de mejora de la calidad, ayudando así a las organizaciones a ascender en la escala de madurez.

Es muy fácil encontrar docenas de variaciones sobre este tema en campos que van desde el desarrollo de software, la adquisición, la ingeniería de sistemas, las pruebas de software, el desarrollo de sitios Web, los Data Warehouse o la ingeniería de seguridad hasta los centros de atención al usuario y la gestión del conocimiento. Evidentemente uno de los modelos más atractivos fue el del kaizen (la mejor forma de mejorar es hacerlo en pequeños pasos).

Después del modelo por etapas de Nolan en 1973, la aplicación más interesante apareció cuando el Instituto de Ingeniería de Software (SEI) de la Universidad Carnegie Mellon publicó su Modelo de Madurez de la Capacidad de Software (SW-CMM), el cual se copió y aplicó en la mayor parte de los casos mencionados anteriormente, convirtiéndose en la práctica en el modelo estándar de madurez. Este modelo fue seguido por nuevas ediciones como CMMI (CMM Integrado).

El modelo de Nolan/Gibson

El modelo de Nolan/Gibson trata de explicar las diferentes etapas de asimilación de las nuevas tecnologías por las organizaciones. Considera que las empresas tienen una cartera de tecnologías de la información diferentes y que cada tecnología pasa a través de las siguientes fases:

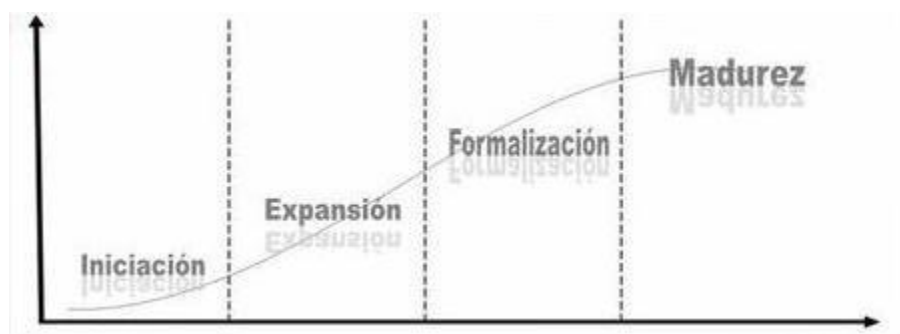
Fase 1: Inversión/proyecto de la nueva tecnología. Esta fase se inicia con la decisión de invertir en una tecnología nueva de tratamiento de la información, que implica el desarrollo de algún proyecto y la formación inicial de las personas. Estos proyectos se caracterizan por su imprecisión presupuestaria, gran incertidumbre y por una gran dosis de aprendizaje.

Fase 2: Aprendizaje de la tecnología y adaptación. Se pretende aprender cómo adaptar la nueva tecnología a unas determinadas tareas más allá de las que se identificaron en la propuesta inicial. Los ciclos de vida del proyecto en esta fase se presentan difíciles para la planificación.

Fase 3: Racionalización/control de gestión. Esta fase trae el desarrollo de controles precisos que guían el diseño e implantación de los sistemas que utilizan estas tecnologías (para asegurar que las aplicaciones posteriores puedan hacerse con mayor eficacia en costes que las primeras).

Fase 4: Madurez/difusión generalizada de la nueva tecnología e integración. Esta fase final puede verse como un programa de difusión tecnológica. Aquí, las empresas recogen la experiencia conseguida en una división operativa y extienden su empleo a toda la firma.

Figura 2: Modelo de Nolan para la Implementación de tecnologías en las organizaciones.



Fuente: <http://sistemas-de-informacion-gerencial.wikispaces.com/Modelo+de+etapas+de+Nolan>

El modelo de Nolan

Es una revisión del modelo de Nolan/Gibson, en el que se habla de 6 fases en lugar de 4. Estas 6 fases son:

Fase 1: Iniciación. Las aplicaciones que se desarrollan tienden a la reducción de costes y se concentran en una función determinada.

Fase 2: Contagio. Todos los departamentos dentro de la organización quieren usar la informática. Ocurre una especie de boom incontrolado donde aparecen una serie de aplicaciones inconexas que duplican inútilmente recursos y funcionalidad.

Fase 3: Control. Debido a la fase anterior, el 80% de la programación se dedica al mantenimiento, con lo que la dirección no ve el resultado de las inversiones. Por ello en esta fase se lleva a cabo una reconstrucción de la actividad informática, con la adopción de controles estrictos en la construcción de aplicaciones. Se hacen menos programas, pero son mejores que los de las etapas anteriores y sirven a la organización para obtener resultados.

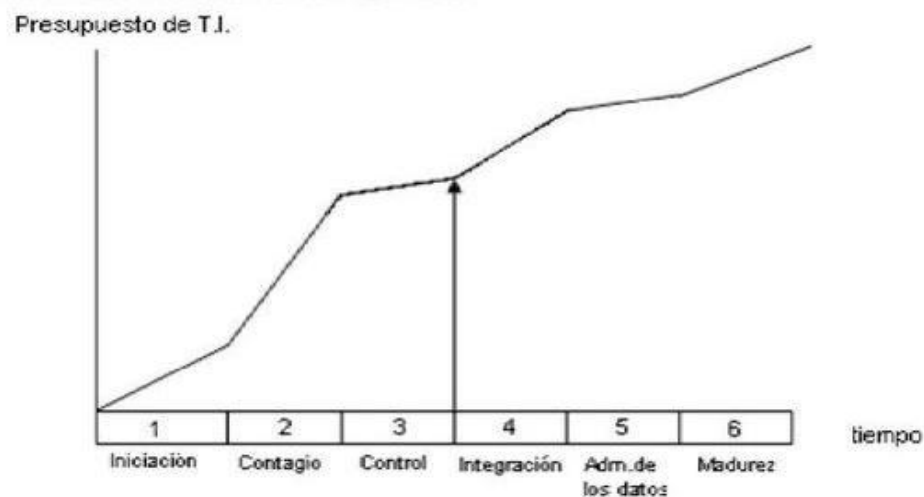
Fase 4: Integración. Los usuarios empiezan a tener un servicio fiable y aprecian el resultado de la implantación del sistema. La dirección se da cuenta de ello y aumenta el gasto en informática.

Fase 5: Administración de datos. Las aplicaciones aisladas dan buen servicio a los usuarios, pero al no estar conectadas provocan un aumento del coste de mantenimiento, tanto de los programas como de la integridad de los datos. En esta fase se modifica la arquitectura interna de la información para reflejar los flujos de información dentro de la empresa.

Fase 6: Madurez. Caracterizada por:

- Integración de todas las aplicaciones de forma que reflejen el flujo de información.
- Eficaz dirección de los recursos informáticos. Planificación estratégica.
- Aceptación de la responsabilidad conjunta de usuarios y de informáticos.

Figura 3: Etapas del modelo de Nolan.



Fuente: [http://sistemas-de-informacion-gerencial.wikispaces.com/Modelo de etapas de nolan](http://sistemas-de-informacion-gerencial.wikispaces.com/Modelo+de+etapas+de+nolan)

El modelo de Gartner¹⁰

Gartner define cinco etapas en las que una organización de TI puede existir: Caótico, Reactiva, Proactivo, Servicio y Valor. En cada etapa la organización de TI se define por

¹⁰ <http://integrared.blogspot.com/2009/07/gartner-fivestage-modelo-de-madurez-de.html>

un conjunto de características. Estas características ilustran los tipos de actividades y comportamientos que se observan en la cultura de la organización.

Chaotic (Caótico)

- No existe documentación
- Infraestructura Impredecible
- No hay procesos comunes o workflow
- Cero monitoreo
- No funcional, no se efectúa planeación o presupuesto.

Reactive (Reactiva)

- Mínima documentación o nada.
- Naciente control de cambio.
- Incentivo a apagar incendios.
- Disponibilidad de solo monitoreo.
- Funcionando, pero sin planeación.

Proactive (Proactivo)

- Documentación de configuración.
- Documentación y aceptación de cambios de control.
- Se Incentiva la planeación sobre incendios.
- Monitoreo de disponibilidad y rendimiento, con predicción de pre-fallas.
- Funcionando, pero tecnología centrada en planeación/presupuesto.

Service (Servicio)

- Documentación de Configuración y SLA.
- Documentación y aceptación de cambios de control.
- Incentivo de servicio de calidad sobre tecnología.
- Monitoreo a nivel de Servicio.
- Funcionando, servicio alineado planeación/presupuesto.

Value (Valor)

- Configuración, SLA, y documentación vinculada al negocio.
- Documentación y aceptación de cambios de control, con vinculación al negocio.

- Incentivo al rendimiento del negocio y calidad de servicio.
- Monitoreo a nivel de Servicio y de Negocio.
- Funcionando, negocio alineado con la planeación/presupuesto.

Figura 4: Estado de madurez de organización en TI.



Fuente: Abast Consulting. Gestión de TI (ITIL, ISO 20000, CobiT).

http://www.abastconsulting.es/gestion_de_ti_itil_iso_20000_cobit.shtml

El modelo de Donovan¹¹

Este modelo, en vez de tomar como variable la inversión realizada en informática, toma como referencia la evolución desde la informática centralizada hacia la descentralizada.

Donovan analiza el proceso tomando tres variables que son:

- El grado en que una organización distribuye el hardware desde su sede central a sus oficinas remotas.

¹¹ Roberto Hernando. Modelo de Nolan.

<http://www.rhernando.net/modules/tutorials/viewtutorial.php?tid=53>

- El grado en que se descentralizan las decisiones referentes a la informática.
- El grado en que se descentraliza la facultad de desarrollar con autonomía nuevas aplicaciones.

Según el valor de estas variables se tienen los siguientes tipos de organizaciones:

- Dinosaurios. Organizaciones con un gran ordenador central, donde las decisiones se toman en la sede central, y todos los programas se gestan en la misma.
- Gran Hermano. Lo único descentralizado es el hardware. Las decisiones y los programas se siguen adoptando y desarrollando en la sede central.
- Mano amiga. Se descentraliza el hardware y las decisiones, permitiendo a los usuarios formar la parte activa. Sin embargo, algunos usuarios avanzados construyen sus propias aplicaciones, con lo que información se dispersa.
- Perro vigilante. Se ha descentralizado el software y el desarrollo de software, pero las decisiones son tomadas desde un organismo central, lo que incluye la adopción de estándares, normas de desarrollo, etc.
- Red o malla. Los tres puntos están descentralizados.

Según Donovan, todas las organizaciones tienden hacia el modelo de malla.

CMMI

CMMI (Capability Maturity Model Integration) es un modelo de madurez de mejora de los procesos para el desarrollo de productos y de servicios. Consiste en las mejores prácticas que tratan las actividades de desarrollo y de mantenimiento que cubren el ciclo de vida del producto, desde la concepción a la entrega y el mantenimiento.

El Modelo de Capacidad y Madurez Integrado (CMMI) es un modelo de referencia de prácticas maduras usadas para evaluar y mejorar la capacidad de los procesos. Es una ruta evolutiva de implementación de las mejores prácticas en los procesos organizacionales.

Este modelo fue desarrollado por el SEI (Software Engineering Institute) de la Universidad Carnegie-Mellon, con un enfoque inicial hacia los procesos relativos al desarrollo de software. Posteriormente se extendió hacia otras temáticas organizacionales, como el desarrollo de proyectos.

Modelos de madurez en CMMI¹²

CMMI propone 5 distintos modelos de madurez de las organizaciones:

Inicial: Estado inicial donde el desarrollo se basa en la heroicidad y responsabilidad de los individuos.

- Los procedimientos son inexistentes o localizados a áreas concretas.

- No existen plantillas definidas a nivel corporativo.

¹² Roberto Canales Mora. Calidad en el desarrollo de Software. CMMI.
<http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=cmmi>

Gestionado: Se normalizan las buenas prácticas en el desarrollo de proyectos (con base en la experiencia y el método). En este nivel consolidado, las buenas prácticas se mantienen en los momentos de estrés.

- Están definidos los productos a realizar.
- Se definen hitos para la revisión de los productos.

Definido: La organización entera participa en el proceso eficiente del proyecto.

- Existen métodos y plantillas bien definidas y documentados.
- Los procesos no solo afectan a los equipos de proyecto sino a toda la organización relacionada.
- Los proyectos se pueden definir cualitativamente.

Cuantitativamente Gestionado:

- Se puede seguir con indicadores numéricos (estadísticos) la evolución de los proyectos.
- Las estadísticas son almacenadas para aprovechar su aportación en siguientes proyectos.
- Los proyectos se pueden medir cuantitativamente.

Optimizado:

- Con base en criterios cuantitativos se pueden determinar las desviaciones más comunes y optimizar procesos.
- En los siguientes proyectos se produce una reducción de costos gracias a la anticipación de problemas y la continua revisión de procesos conflictivos.

PLAN DE CONTINGENCIA INFORMÁTICA

Definición

El Plan de Contingencia Informática es un instrumento de gestión que contiene las medidas técnicas, humanas y organizativas para que una organización garantice la continuidad de la operación en caso de cualquier incidente o situación que impida la operación habitual de la plataforma informática. Esta herramienta requiere la identificación de aquellos sistemas de información y/o recursos de TIC's críticos que son susceptibles de riesgo de deterioro, violación o pérdida, ya sea por causa física o humana, con el propósito de estructurar y ejecutar procedimientos y asignar responsabilidades que salvaguarden la información y permitan su recuperación garantizando la confidencialidad, integridad y disponibilidad de ésta, en el menor tiempo posible, a unos costos razonables y minimizando las pérdidas.¹³

El plan de contingencia tiene un carácter reactivo, es decir, es utilizado únicamente cuando ya ha ocurrido un desastre. Esta es la diferencia básica comparándolo con el plan de continuidad, pues este último, aparte de tener medidas en caso de desastre

¹³ Alonso Tamayo Alzate, Johnny Tamayo. Guía para la formulación de un Plan de Contingencias Informáticas, diseñada y aplicada desde las aulas de clase de la Universidad Nacional de Colombia - sede Manizales. <http://www.cibersociedad.net/congres2006/gts/comunicacio.php?id=309>

también analiza las vulnerabilidades y desarrolla alternativas para mitigar dichas vulnerabilidades, es de carácter preventivo y pretende alcanzar una disponibilidad de 99.999% para la infraestructura crítica, lo que implica que el sistema siempre esté disponible. El plan de continuidad no es excluyente del plan de contingencia, en realidad el segundo está incluido en el primero.

De acuerdo a las necesidades particulares, cada organización decide implementar mecanismos para enfrentar el reto de la seguridad de la información. Algunas empresas emprenden el gran proyecto de la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) generalmente apoyándose en la norma ISO 27001 y en la guía de buenas prácticas ISO 27002 que son un conjunto de estándares que proporcionan un marco de gestión de la seguridad de la información. Estas sirven como guía metodológica para diseñar los controles necesarios para proteger los activos de información, basada en el análisis de riesgos, buscando implementar, establecer, operar, monitorear, revisar, mantener y mejorar la seguridad de la información en cualquier empresa. Esta decisión requiere un fuerte compromiso de la alta dirección de la empresa y demanda una alta asignación de recursos.

Otra alternativa resulta cuando se decide trabajar sólo algunos aspectos de seguridad, evaluando riesgos y generando un plan de continuidad de negocio, lo cual resulta más económico; Sin embargo, esta opción aún es costosa y no todas las empresas tienen los recursos para abordar este proyecto, incluso algunas empresas deciden desarrollar el plan de continuidad sólo para algunos de sus procesos más críticos. Teniendo en cuenta estas consideraciones, generalmente las pymes, aceptan asumir el riesgo de no contar con un plan de continuidad y se concentran en elaborar un plan de contingencia.

Consideraciones de implementación

Toda organización debe planear y desarrollar un Plan de Contingencia cuando todavía no es necesario, es decir, antes de que los eventos ocurran. La planificación aumenta la habilidad y capacidad de la organización para “sobrevivir” y mantener las operaciones en caso de incidentes o desastres, sirviendo como punto de partida y aportando una guía de acciones que se deben ejecutar para una adecuada respuesta en caso de emergencia.

El Plan de Contingencia debe cubrir todos los aspectos que se van a adoptar tras una interrupción, lo que implica suministrar el servicio alternativo y para lograrlo no solo se deben revisar las operaciones cotidianas, sino que también debe incluirse el análisis de los principales componentes de la infraestructura en riesgo. Esto incluye cubrir los siguientes puntos: hardware, software, documentación, talento humano y soporte logístico; debe ser lo más detallado posible y fácil de comprender.

Los responsables de la planificación, deben evaluar frecuentemente los planes creados, así como analizar otras situaciones que se pudieran llegar a presentar. Un Plan de Contingencia estático se queda rápidamente obsoleto y produce una falsa sensación de seguridad, por lo cual debe ser un documento “vivo”, actualizándose, corrigiéndose, y mejorándose constantemente, de manera que se pueda confiar en que las medidas adoptadas son apropiadas y pertinentes. También es necesario considerar como será divulgado.

Un Plan de Contingencia debe ser exhaustivo, evitando entrar en demasiados detalles; debe ser de fácil lectura, cómodo de actualizar, y debe ser una guía operativa clara y precisa. En síntesis, debe decir qué hay que hacer, quién, cuándo y cómo.

El Plan de Contingencia debe tener en cuenta al personal que participa en su implementación y aquellos que participarán operativamente en el momento en que se

presente un incidente y el plan deba ejecutarse. Este debe detallar los nombres de los encargados de la contingencia y sus responsabilidades.

Etapas para elaborar un Plan de Contingencia

Las etapas básicas para elaborar el Plan de Contingencia informática de una organización son: ¹⁴

Análisis y valoración de riesgos

En primer lugar se debe realizar un análisis del impacto que causaría en la organización una falla e incidente en la plataforma tecnológica o un desastre natural. Se identifican los procesos críticos y las consecuencias que se presentan en caso de no estar en funcionamiento. El primer componente del Plan de Contingencia debe ser una descripción del servicio y el riesgo para ese servicio. También es recomendable determinar el costo que representa para la organización experimentar estos incidentes.

La evaluación del nivel de riesgo de la información sirve para:

- Determinar la relación costo/beneficio y tener argumentos para decidir entre aceptar la pérdida de información o invertir en implementar sistemas de contingencia.
- Clasificar los componentes de la plataforma tecnológica en términos de riesgo (alto, medio, bajo) e identificar aquellos que representen mayor riesgo.
- Cuantificar el impacto en el caso de suspensión del servicio.

¹⁴ Alonso Tamayo Alzate, Johnny Tamayo. Guía para la formulación de un Plan de Contingencias. <http://www.cibersociedad.net/congres2006/gts/comunicacio.php?id=309>

- Determinar la información que pueda representar pérdidas considerables para la organización o que impida una adecuada toma de decisiones.

Este análisis de posibles riesgos permitirá identificar las fortalezas, oportunidades, debilidades y amenazas, y profundizar en las medidas que se deben tomar para gestionarlas, de manera que en caso de incidentes se pueda recuperar la operatividad en el menor tiempo posible.

Jerarquización de las aplicaciones

Es indispensable definir con anticipación cuáles son las aplicaciones primordiales para la organización. Teniendo en cuenta que para cada departamento o área funcional de la organización, su operación es la más importante, la jerarquización debe estar avalada y respaldada por un comité de contingencia o por la alta dirección, procurando objetividad y minimizando el conflicto de intereses.

El plan debe incluir una lista de los sistemas, aplicaciones y prioridades, así como identificar aquellos elementos informáticos (hardware, software base, software de aplicaciones, telecomunicaciones) que puedan ser críticos ante cualquier incidente o desastre, jerarquizándolos de acuerdo al orden de importancia dentro de la organización. Se deben incluir los problemas generados por ausencia de fuentes de energía, mala administración o uso de dispositivos de backup o cualquier otro daño de origen físico que pueda provocar la pérdida masiva de información.

Establecimiento de requerimientos de recuperación

Esta etapa busca determinar lo que se debe hacer para lograr una óptima solución, especificando las funciones con base en el estado actual de la organización. Es necesario realizar las siguientes actividades: profundizar la definición del problema, analizar áreas o componentes problema, comunicaciones y sus flujos, formulación de

medidas de seguridad necesarias dependiendo del nivel de seguridad requerido, justificación del costo de implantar las medidas de seguridad, análisis y evaluación del plan de contingencia actual (si lo hay), determinar los recursos humanos, técnicos y económicos necesarios para desarrollar el plan, definir un tiempo prudente y viable para lograr que el sistema se libere y pueda entrar en operación.

Ejecución

Una vez finalizado el plan, es conveniente elaborar un informe final con los resultados de su ejecución cuyas conclusiones pueden servir para mejorar éste ante eventualidades que se puedan presentar con posterioridad. En esta etapa se debe tener presente que el plan de contingencia no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas de la empresa.

Para garantizar el éxito del plan de contingencia es conveniente que en su elaboración participen la alta dirección de la organización, personal técnico y operativo de los procesos y los usuarios, ya que los recursos necesarios para la puesta en marcha del plan, demandan mucho esfuerzo técnico, económico y organizacional y se requiere observar el sistema, la plataforma tecnológica y la operación de la compañía desde diversos puntos de vista.

Pruebas y simulaciones

Es necesario definir y generar simulaciones que permitan poner a prueba el plan de contingencia, el personal y los recursos necesarios para su realización. El propósito es intentar valorar el impacto real de un problema dentro de los escenarios establecidos como posibles. En caso de que los resultados obtenidos difieran de los esperados, se debe analizar si el resultado varió por un problema en el ambiente de pruebas del plan, en cuyo caso se podrá corregir el problema y repetir la prueba, ó si el plan tiene vacíos o carencias en su definición. Es indispensable la capacitación y

participación del equipo de contingencia para detectar y evidenciar posibles carencias del plan, así como una buena documentación para facilitar la ejecución de las pruebas.

Documentación

Aunque esta etapa demanda un esfuerzo significativo, ayudará a comprender otros aspectos del sistema y puede ser apoyo para la empresa en caso de ocurrir un incidente o desastre. Debe incluir los procedimientos detallados que expliquen el paso a paso de las tareas de instalación y recuperación necesarias, procurando que sean entendibles y fáciles de seguir.

La documentación del plan de contingencia se debe desarrollar a medida que se avanza en la definición del plan y desde el mismo momento que nace, pasando por todas sus etapas; en ningún caso se debe dejar de lado esta labor, esperando a realizarla cuando se concluyan las pruebas y su difusión, pues se correría el riesgo de que la documentación resulte inexacta, difusa y que cualquier aspecto importante se pase por alto.

Difusión y mantenimiento

Con el plan de contingencia probado y documentado, surge la necesidad de su difusión y capacitación entre las personas encargadas de llevarlo a cabo. El mantenimiento del plan comienza con una revisión del plan existente y se examina en su totalidad realizando los cambios en la información que pudo haber ocasionado una variación en el sistema y realizando los cambios que sean necesarios. La generación del plan no muere aquí, por el contrario es el inicio de un ciclo de revisión, ajuste y divulgación constante que suministre a la organización la tranquilidad de estar preparada y lista ante cualquier incidente.

Norma ISO 27001, Guía de buenas prácticas ISO 27002 y necesidad del Plan de Contingencia

La norma ISO 27001¹⁵ es un estándar internacional diseñado por la ISO/IEC (Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional, que busca proporcionar un modelo para establecer, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). El diseño e implementación de un SGSI debe corresponder a las necesidades de la organización, de manera que se proporcionen los controles de seguridad que protejan los activos de información y que aporten confianza a las partes interesadas.

La Norma ISO 27001 plantea el modelo PDCA (Plan – Do – Check – Act), en español, PHVA (Planear – Hacer- Verificar – Actuar), que las organizaciones deben seguir como metodología para gestionar el SGSI. De esta manera la norma ISO 27001 define que la organización debe:

Planear

- Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología.
- Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología.
- Definir el enfoque de valoración del riesgo de la organización
- Identificar los riesgos
- Analizar y evaluar los riesgos

¹⁵ Estándar Internacional ISO/IEC 27001 Primera Edición 2005

- Identificar y evaluar las opciones para el tratamiento de los riesgos
- Seleccionar objetivos de control y controles para el tratamiento de los riesgos
- Obtener la aprobación de la Gerencia para los riesgos residuales propuestos
- Obtener la autorización de la Gerencia para implementar y operar el SGSI
- Preparar un enunciado de aplicabilidad

Hacer

- Formular un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.
- Implementar el plan de tratamiento de riesgo para lograr los objetivos de control, incluyendo asignación de roles y responsabilidades
- Implementar los controles seleccionados para satisfacer los objetivos de control
- Definir los mecanismos para medir la efectividad de los controles
- Implementar programas de capacitación y conocimiento
- Manejar las operaciones del SGSI
- Manejar recursos para el SGSI

- Implementar procedimientos y controles capaces de permitir detectar y responder oportunamente a incidentes de seguridad

Verificar

- Ejecutar procedimientos de monitoreo y revisión para detectar errores en resultados de procesamiento, identificar incidentes, eventos y violaciones de seguridad, determinar la efectividad de las acciones tomadas para resolver estas fallas.
- Realizar revisiones periódicas de la efectividad del SGSI y de los controles de seguridad.
- Medir efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad
- Revisar las evaluaciones del riesgo, nivel de riesgo residual, y riesgo aceptable tomando en cuenta cambios en la organización, la tecnología, los objetivos y proceso comercial, nuevas amenazas, efectividad de los controles, y regulaciones, leyes, contratos.
- Realizar auditorías internas al SGSI
- Realizar una revisión gerencial del SGSI
- Actualizar los planes de seguridad teniendo en cuenta los resultados de las actividades de monitoreo y evaluación
- Registrar acciones y eventos que podrían tener impacto en la efectividad o desempeño del SGSI.

Actuar

- Implementar las mejoras identificadas en el SGSI
- Tomar acciones preventivas y correctivas
- Aplicar lecciones aprendidas de las experiencias de seguridad de otras organizaciones y de la organización misma.
- Comunicar resultados y acciones a todas las partes interesadas.
- Asegurar que las mejoras logren los objetivos.

Por su parte la ISO 27002:2005¹⁶ es una guía de buenas prácticas de seguridad de la información que presenta los objetivos de seguridad que sería ideal alcanzar, una extensa serie de controles a tener en cuenta para cada objetivo y un conjunto de sugerencias o recomendaciones para cada control. Esta guía comprende 11 dominios, 39 objetivos de control y 133 controles.

Los 11 dominios son:

- Política de seguridad
- Aspectos organizativos de la seguridad de la información
- Gestión de Activos
- Seguridad ligada a los Recursos Humanos

¹⁶ ISO 27002. <http://www.iso27002.es/>

- Seguridad Física y del entorno

- Gestión de comunicaciones y operaciones

- Control de acceso

- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

- Gestión de Incidentes en la Seguridad de la Información

- Gestión de la Continuidad del Negocio

- Cumplimiento

El propósito de la norma 27001 es que la organización determine cuáles son sus requerimientos, defina un alcance de lo que desea implementar y aborde los controles necesarios para satisfacer sus necesidades de seguridad. En ningún caso la guía de buenas prácticas ISO 27002 debe considerarse como un listado de controles que la organización está obligada a alcanzar para lograr la estandarización, y por ende la certificación ISO 27001.

Los planes de contingencia surgen entonces a partir de la necesidad de las organizaciones de mantener la continuidad de los sistemas de información frente a eventos o incidentes, atendiendo los dominios de Gestión de incidentes en la seguridad de la información y la Gestión de la Continuidad del negocio.

MODELO DE GOBIERNO TI BASADO EN COBIT¹⁷

Creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992.

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT por sus siglas en inglés: Control Objectives for Information and related Technology) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

- Estableciendo un vínculo con los requerimientos del negocio.
- Organizando las actividades de TI en un modelo de procesos generalmente aceptado.
- Identificando los principales recursos de TI a ser utilizados.

¹⁷ ISACA. COBIT 4.1. <http://www.isaca.org>.

- Definiendo los objetivos de control gerenciales a ser considerados.

La orientación al negocio que enfoca COBIT consiste en alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

Figura 5: Áreas de enfoque del gobierno de TI.



Fuente: <http://cafrancavilla.wordpress.com/tag/problemas-it/>

- **Alineación Estratégica:** se enfoca en garantizar la alineación entre los planes de negocio y de TI, en definir, mantener y validar la propuesta de valor de TI, y en alinear las operaciones de TI con las operaciones de la empresa.

- **Entrega de Valor:** se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.

- **Administración de Recursos:** se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI: aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.

- **Administración de Riesgos:** requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del apetito de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

- **Medición del Desempeño:** rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas medibles más allá del registro convencional.

ESTÁNDAR PARA LA GESTIÓN DE SERVICIOS INFORMÁTICOS ITIL

La Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) fue desarrollada en 1980 por la CCTA (Agencia Central de Telecomunicaciones), buscando estandarizar la operación de todos los proveedores de tecnología (internos y externos) para el gobierno del Reino Unido. El resultado fue una guía que esta formada por una serie de “Mejores prácticas” procedentes de todo tipo de suministradores de servicios de TI.¹⁸

ITIL especifica un método sistemático que garantiza la calidad de los servicios de TI. Ofrece una descripción detallada de los procesos mas importantes en una organización de TI, incluyendo listas de verificación para tareas, procedimientos y responsabilidades que pueden servir como base para adaptarse a las necesidades de cada organización.

ITIL pertenece a la OGC (Oficina de comercio gubernamental), entidad que en 2001 absorbió a la CCTA, pero es de libre utilización.

En junio de 2007, la OGC publicó la última actualización a ITIL, conocida comúnmente como ITIL V3. Esta consta de 5 libros basados en el ciclo de vida del servicio: Estrategia del Servicio, Diseño del Servicio, Transición del Servicio, Operación del Servicio, Mejora Continua del Servicio.

A lo largo de todo el ciclo de los productos TI, la fase de operaciones alcanza cerca del 70% al 80% del total del tiempo y de los costos, el resto se invierte en el desarrollo de productos o servicios. De esta manera, los procesos eficaces y eficientes de la Gestión de Servicios TI se convierten en esenciales para el éxito de los departamentos de TI. Esto se aplica a cualquier tipo de organización, grande o pequeña, pública o privada, con servicios TI centralizados o descentralizados, con servicios TI internos o

¹⁸ http://itil.osiatis.es/Curso_ITIL/

suministrados por terceros. En todos los casos, el servicio debe ser fiable, consistente, de alta calidad, y de costo aceptable.

El ciclo de vida ITIL

El ciclo de vida ITIL, consta de cinco fases, cada una con sus respectivas funciones y procesos, que indican la manera de implementar las mejores prácticas, con el fin de obtener un servicio TI de alta calidad. Estas fases son:¹⁹

- **Estrategia del servicio:** esta fase del ciclo de vida ITIL, define directrices para el diseño, desarrollo e implantación de la gestión del servicio como un recurso estratégico. Es fundamental en el contexto de los procesos que se siguen en las otras fases del ciclo de vida del servicio. Su principal función es mejorar la sincronización entre TI y las estrategias empresariales.
- **Diseño del servicio:** se ocupa del diseño y desarrollo de servicios y sus procesos relacionados. Afecta tanto a los nuevos servicios, como a los que han sido modificados. Entre sus objetivos están: contribuir con los objetivos del negocio, ahorrar (en lo posible) tiempo y dinero, minimizar riesgos y evaluar y mejorar la eficiencia de los servicios de TI.
- **Transición del servicio:** convierte las especificaciones de la fase anterior, en un servicio nuevo o modificado, reduciendo las variaciones en el rendimiento y los errores conocidos y garantizando que este cumple con los requisitos del negocio. Para lograr esto, se vale de los siguientes pasos: planificación y preparación, construcción y pruebas, pilotos, y planificación y preparación del despliegue.

¹⁹ Tieneke Verheijen, Annelies van der Veen, Ruby Tjassing, Mike Pieper, Axel Kolthof, Arjen de Jong, & Jan van Bon. (2010). Fundamentos de ITIL V3. Van Haren publishing.

- **Operación del servicio:** tiene como objetivos la coordinación y ejecución de las actividades y procesos necesarios para entregar y gestionar servicios para usuarios y clientes con el nivel especificado. También tiene la responsabilidad de gestionar la tecnología necesaria para la prestación y el soporte de los servicios.
- **Mejora continua del servicio:** se centra en las actividades que mejoran la calidad del servicio. Para esto utiliza el ciclo “Planear, hacer, verificar actuar”, que establece una fase de consolidación para cada mejora, con el fin de incorporar nuevos procedimientos en la organización. Las medidas y análisis son muy importantes, ya que permiten identificar los servicios rentables y aquellos que se pueden mejorar.

Figura 6. Ciclo de vida ITIL.



Fuente: Secure and IT proyectos. ITIL / ISO 20000.

<http://www.secureit.es/index.php?page=seguridad&subpage=iso20k>

CAPITULO 1

1. ANÁLISIS Y DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DEL DEPARTAMENTO DE SISTEMAS Y SU ROL EN LA ORGANIZACIÓN.

1.1. Evaluación de la madurez de TIC en la empresa “T”

Esta evaluación de madurez intenta determinar el estado actual de las TIC al interior de la organización, haciendo uso del modelo Nolan adaptado por Fredy Reyes. Las calificaciones se obtuvieron ponderando los resultados de la encuesta a usuarios finales (Ver Anexo 1), visita a las instalaciones de la compañía y entrevista con los miembros del Departamento de Sistemas. Estas herramientas permitieron la clasificación de las tecnologías usadas por la compañía, para su análisis individual.

1.1.1. Tecnologías

T1	Equipos de informática y software básico
T2	Comunicaciones y redes
T3	Sistemas de información (JDE, Zue, CIO)
T4	Infraestructura de servidores

Evaluación de las tecnologías

➤ Equipos de informática y software básico

Número	Criterio	Calificación
1	Grado de cubrimiento en la organización	4
CR2	Dominio de los usuarios	3
CR3	Soporte del área informática	4
Total		3.67

➤ Comunicaciones y redes

Número	Criterio	Calificación
CR1	Grado de cubrimiento en la organización	3
CR2	Dominio de los usuarios	2
CR3	Soporte del área informática	3
Total		2.67

➤ Sistemas de información

Número	Criterio	Calificación
CR1	Grado de cubrimiento en la organización	3
CR2	Dominio de los usuarios	3
CR3	Soporte del área informática	3

Total	3
--------------	----------

➤ Infraestructura de servidores

Número	Criterio	Calificación
CR1	Grado de cubrimiento en la organización	4
CR2	Dominio de los usuarios	3
CR3	Soporte del área informática	3
Total		3.33

Evaluación del soporte a la gestión de los sistemas de información:

Número	Criterio	Calificación
CR1	Estratégico	4
CR2	Táctico	4
CR3	Operativo	3
CR4	Integración	3
Total		3.5

Conclusión Tecnologías

Tecnologías	Calificación
--------------------	---------------------

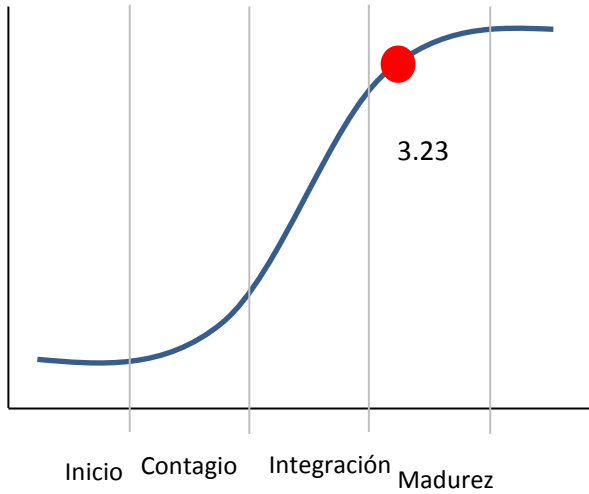
Equipos de informática y software básico	3.67
Comunicaciones y redes	2.67
Sistemas de información (JDE, Zue, CIO)	3
Infraestructura de servidores	3.33
Soporte a la gestión de los sistemas de información	3.5
Total	3.23

La conclusión a que se llega en la evaluación de las tecnologías, ubica a la organización entre las etapas de “Integración de la información” y “Madurez”, con una tendencia cercana a la primera.

En general, es notorio el interés de la organización por implementar tecnologías de información y comunicación que apoyen y cubran en alto grado todas las actividades tácticas y operativas, con el fin de mejorar la operación y brindar valor tanto a los usuarios internos, como a los clientes externos. Los usuarios en general tienen un buen grado de aceptación y dominio de las tecnologías que apoyan sus labores, pero se notan debilidades en el uso de las comunicaciones y redes, porque se desconoce el uso y las bondades adicionales que éstas pueden ofrecer.

El soporte del área de Sistemas tiene una buena calificación, pero la falta de metodologías impide un cubrimiento total y evidencian un sentimiento de retraso en las tareas de soporte por parte de los clientes internos. La parte operativa y administrativa de las tecnologías es atendida por dos funcionarios que tienen bajo su responsabilidad atender los soportes y requerimientos solicitados por los demás usuarios, impidiendo que se dedique tiempo a actividades de evaluación e investigación de nuevos usos tecnológicos o a la explotación de los que ya existen, lo que le da un carácter al área más reactivo que proactivo.

Figura 1.1. Curva de Nolan adaptado por Fredy Reyes resultado de la calificación de las tecnologías.
Fuente: Los autores.



1.1.2. Motivaciones de la organización hacia la informática

Figura 1.2: Curva de Nolan adaptado por Fredy Reyes resultado de la calificación de las Motivaciones de la organización hacia la informática. **Fuente:** Los autores.



La organización tiene una motivación “Ofensiva” frente a las TIC. Tanto para los líderes de área, como para los usuarios en general, las herramientas tecnológicas ofrecen un medio que facilita la realización de las actividades y apoya la toma de decisiones.

El sistema de información corporativo es un ERP que al ser empleado correctamente permite alto grado de integración, lo que permite un flujo oportuno y confiable de la información, que apoya la gestión de los diferentes departamentos, apoyando el crecimiento y la expansión de la empresa.

Los usuarios encuestados en los diferentes niveles, no ven la tecnología de la compañía como una herramienta que les permita alcanzar un mayor nivel de competitividad frente a las demás empresas del sector, lo que indica que la motivación de la organización debe centrar sus esfuerzos en conseguir y promover tecnologías que permitan adicionar valor al cliente externo, de manera que se perciba un factor diferenciador que ayude al posicionamiento de la empresa en su área de negocio.

1.1.3. Nivel de participación y asimilación de las TIC por los usuarios

Número	Criterio	Calificación
CR1	Promotores del uso de TIC	3
CR2	Integración de usuarios en los servicios de TIC	2
CR3	Habilidad para la gestión de la información	3
CR4	Nivel de resistencia al cambio	3
Total		2.75

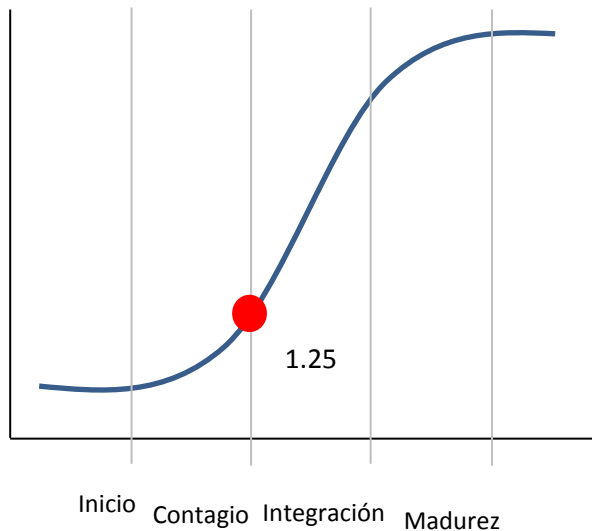
La participación y asimilación de las TIC de acuerdo a la opinión de los usuarios encuestados tanto en los rangos operativos como en los líderes de área, es buena. Es común que las personas al interior de la organización estén interesadas en incluir las TIC como herramientas para su trabajo, porque han entendido todos los beneficios que éstas ofrecen.

Un punto crítico en la definición de requerimientos es la falta de cultura para realizar las solicitudes. Los usuarios hacen requerimientos ambiguos o no realizan un análisis consciente previo a la solicitud, por lo que terminan solicitando cosas que realmente no necesitan y solo hasta el momento de la entrega definen sus necesidades reales.

1.1.4. Metodologías y procedimientos

Criterio	Calificación
Uso de metodologías y procedimientos en los diferentes procesos de TI	1
Uso de Procedimientos Externos a la GI	2
Evaluación de Desempeño de la GI	1
Adopción de Herramientas de Gobernabilidad en TIC.	1
Total	1.25

Figura 1.3. Curva de Nolan resultado de la calificación de las metodologías y procedimientos. **Fuente:** Los autores.



En el uso de metodologías y procedimientos en el área de TI, la Compañía y el Departamento de Sistemas se encuentran en un nivel bajo, producto de la inexistencia de herramientas y procesos de gobernabilidad de TIC que permitan un marco de referencia para el trabajo.

La empresa se encuentra certificada en la norma ISO 9001:2008, lo que motivó que el Departamento de Sistemas definiera un procedimiento para la realización de backups y creación de usuarios, que elevan la calificación por el uso de procedimientos externos, pero que no son suficientes y que al no tener un enfoque propio en TI, no contribuyen en las labores propias de la Gerencia informática.

La ubicación de la calificación cercana a la etapa de inicio, indica que se deben realizar esfuerzos para la implementación de metodologías de TI y procesos de gobernabilidad que permitirán un mejor flujo de las acciones del área informática y una orientación al logro de las actividades que aportan valor estratégico a los objetivos corporativos.

1.1.5. Carácter de la gerencia informática

Criterio	Calificación
Posición de la Gerencia de TIC en la estructura orgánica	1
Nivel de liderazgo del Gerente informático en la organización	N/A
Capacidad de alineación e interdependencia de la estrategia de TIC con la estrategia organizacional	3
Capacidad de gestión de servicios tercerizados de TIC	3
Capacidad del talento humano de GI en aspectos técnicos	4
Capacidad del talento humano de GI en gerencia de proyectos	2
Capacidad del talento humano de GI en gestión de servicios (al cliente interno)	4
Total	2.83

La ubicación del Departamento de sistemas en la estructura orgánica de la empresa, dependiendo de un área no técnica, así como la falta en el momento actual de un Gerente informático, son factores que impiden la gobernabilidad de TIC y por ende el buen desarrollo y la orientación de TI.

El personal de esta área posee un nivel adecuado de conocimientos técnicos, pero la carencia de metodologías para la gestión de proyectos relega su participación al plano operativo.

La tercerización de servicios como el alojamiento de servidores fuera de las instalaciones físicas de la empresa, y la administración y mantenimiento de éstos,

demuestran el interés del área en delegar en externos especializados las actividades que siendo neurálgicas para la compañía, requieren un cuidado específico que por falta de recursos, como tiempo y personal capacitado, no se pueden realizar al interior de la organización. Esta transferencia de actividades libera tiempo para la Gerencia de TI, que puede ser utilizado en otras que no es adecuado delegar.

Además de los conocimientos específicos de TI, los responsables del soporte tienen una muy buena calificación por parte de todos los usuarios en el aspecto del servicio, lo que da un valor adicional a las actividades y genera confianza en su trabajo.

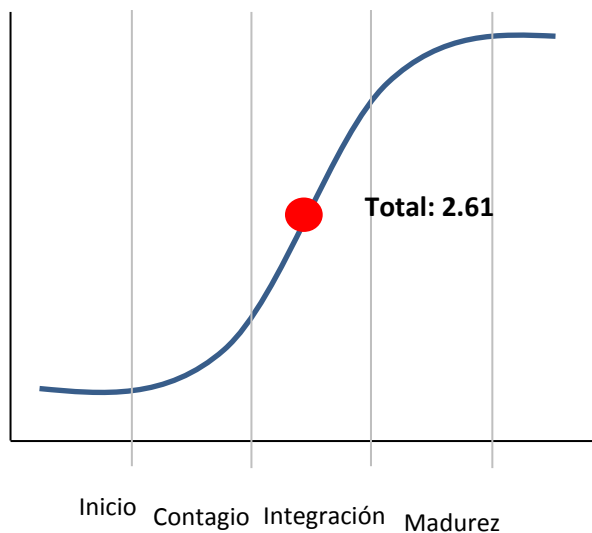
1.1.6. Conclusión final

Ítem	Indicador	Calificación
CR1	Tecnología	3.23
CR2	Motivaciones de la organización hacia la informática	3
CR3	Participación y asimilación de los usuarios en las TIC	2.75
CR4	Metodologías y procedimientos	1.25
CR5	Carácter de la gerencia informática	2.83
Total		2.61

La calificación de madurez informática de la Empresa T, la ubica entre las etapas de contagio e integración, con una leve mayor cercanía hacia la segunda. La tabla que ilustra la conclusión final, muestra que la empresa es fuerte en el uso de la tecnología, y que la adopta como un factor estratégico. Esto se evidencia también en el interés por invertir en sistemas informáticos y en la plataforma tecnológica, y en la percepción que se tiene de las TIC como factor decisivo para la competitividad y el desarrollo corporativo.

El criterio número 3 que tiene una calificación cercana a la mitad, indica que los usuarios comprenden la importancia de las TIC y las asimilan como medios para la realización de su trabajo, pero no explotan por completo su capacidad, en parte porque se centran exclusivamente en su día a día laboral y no se interesan en obtener conocimientos diferente a los de su actividad cotidiana.

Figura 1.4. Curva de Nolan adaptado por Fredy Reyes resultado de la evaluación de madurez informática. **Fuente:** Los autores.



El aporte que tienen los usuarios en la planificación de TIC, resta puntos en la calificación de este ítem, debido a dos circunstancias: la falta de metodologías al interior de la empresa que permitan e incentiven una participación efectiva y contundente, y el prejuicio cultural común en el medio, que restringe las actividades de planeación y ejecución de proyectos de TI solo a los ingenieros.

El punto más crítico en la evaluación de madurez de la compañía, es el criterio número 4, que baja de manera importante la calificación total, y se nota como el factor más relevante que se debe corregir. Le sigue en aspecto crítico, la falencia de

metodologías y prácticas de gobernabilidad y la dependencia de un departamento de enfoque administrativo.

Esta evaluación despeja algunas estrategias que podrían implementarse para corregir los puntos en los que la organización no es totalmente efectiva, y subir la calificación de madurez con el fin de mejorar los logros resultantes de la gestión de las TIC.

- Crear un punto de contacto directo entre los usuarios y el personal de TI, que permita canalizar los requerimientos y priorizarlos. Se requiere cambiar la cultura para la realización de solicitudes, fomentar la participación de los usuarios y buscar la optimización en el uso de herramientas tecnológicas.
- Fortalecer los procedimientos con la utilización de nuevas herramientas y prácticas que permitan asegurar la operación y la continuidad del negocio.
- Implementar prácticas de metodologías como ITIL, CMMI y COBIT, que permitan encaminar las labores del Departamento de Sistemas, hacia la obtención de mejores resultados, aprovechando los recursos con que ya se cuenta.
- Fortalecer el carácter del área de TI, reestructurándola desde el interior y ubicándola en una posición más autónoma y estratégica dentro de la organización, que le permita mayor agilidad en la toma de decisiones y entrega de resultados. Esto adicionalmente debe posicionar en la compañía las tecnologías de información y comunicación, como herramientas para la competitividad en el sector.

1.2. Revisión de los procesos actuales del departamento de sistemas en la empresa “T”

1.2.1. Procesos de gestión de los sistemas de información

- **Desarrollo y Mantenimiento del Sistema de Información:** El área se encarga de la gestión y análisis de requerimientos (modificaciones a la configuración del ERP, desarrollo de reportes y aplicaciones) que solicitan los usuarios, correcciones de errores del software y ajustes o nuevos desarrollos para adaptar el sistema a las necesidades del negocio. Efectúa el diseño y análisis de las soluciones, desarrollo de código o programación, realiza las pruebas o verificación del software, y luego, libera el resultado o software a ambiente de producción.
- **Administración de Implantación de Software:** El Departamento de Sistemas gestiona cualquier instalación, implementación o actualización ejecutada sobre los sistemas de información (ERP, software de nómina, software de presupuestos, etc. El propósito es asegurar que la implantación de software soporta las necesidades de la compañía y que el nuevo software o las actualizaciones sobre uno ya existente no alterarán el desempeño normal de la operación.

La gestión de software también incluye la instalación y actualización de otros programas y aplicaciones como sistemas operativos, paquetes de oficina (Microsoft Office), programas de diseño (Autocad, visores de CAD), programas para gestión de proyectos, y cualquier otro tipo de software.

También incluye actividades realizadas para el control de licenciamiento e inventario de software.

- **Soporte del Sistema de Información:** El área se encarga de brindar soporte técnico al usuario sobre los módulos del sistema de información corporativo (ERP

JDEdwards). También presta un servicio de soporte funcional básico. En caso de que se requiera un soporte más avanzado, se gestiona una solicitud de servicio mediante un sistema de servicio al cliente ante el partner del fabricante del software en Colombia.

- **Administración de la Operación del Sistema de Información:** Es responsabilidad del área velar por la disponibilidad y correcta operación del sistema. Esto incluye instalación periódica de paquetes de software, revisión de servicios, administración y mantenimiento de las Bases de Datos, revisión y administración de desempeño y carga de los recursos de los servidores, generación de backups, gestión de seguridades del Sistema, administración de usuarios y perfiles.

1.2.2. Procesos de gestión de infraestructura de TI

- **Selección, contratación y/o compra de Infraestructura:** Con base en las necesidades detectadas y de acuerdo a aprobación de la Dirección, el área se encarga de buscar proveedores, solicitar cotizaciones, comparar propuestas, elegir proveedor y tramitar ante el área de Compras de la compañía la generación de ordenes de compra o servicio y los anticipos que se requieran. También se realiza el recibo del producto o servicio, verificando su calidad y cumplimiento de lo comprado/contratado, y se efectúa aprobación de las facturas para que el área financiera efectúe el pago.

También se realiza seguimiento de proveedores y del producto o servicio, y en caso de ser necesario se tramitan las garantías o se gestionan las inconformidades por incumplimiento en los niveles de servicio del proveedor.

- **Instalación y Administración de Infraestructura de TIC:** El área se encarga de la instalación, configuración y administración de hardware (equipos de cómputo, impresoras, escáneres, teléfonos, equipos de redes y comunicaciones). En otros

casos, se contratan terceros que prestan un servicio (canales de comunicaciones, telefonía, hosting de servidores, etc.) y es responsabilidad del área velar por el correcto funcionamiento de estos servicios, y en caso de fallas gestionar que el tercero realice las revisiones y ajustes correspondientes, garantizando continuidad del servicio y disponibilidad de los recursos para los usuarios. También se realiza administración del inventario y control de las hojas de vida de los equipos.

- **Soporte Técnico:** El área se encarga de las actividades de mantenimiento preventivo y correctivo de equipos, y tareas de help desk para apoyar las necesidades y resolver las consultas de los usuarios en el uso de herramientas tecnológicas. Se brinda soporte telefónico, por mensajería instantánea, control remoto y soporte presencial.
- **Administración de la Seguridad Informática:** El área debe velar por la protección de los recursos informáticos y en general, la información de la compañía. Para esto, define los controles y mecanismos para administrar la seguridad de la información. Esto incluye gestión de la red, gestión del permisos de los usuarios y perfiles, administración de la seguridad de los servidores y del sistema de información.

También incluye la gestión de copias de respaldo (backups) de la información contenida en las bases de datos de los sistemas de Información, el servidor de archivos y los equipos de cómputo de los cargos estratégicos de la compañía.

1.2.3. Procesos de planeación de TIC

- **Propuestas de Mejoramiento:** Con base en la observación de las necesidades de la compañía y el desempeño de la infraestructura de TI, el área propone alternativas de mejoramiento, justificando la inversión o recursos requeridos.

- **Elaboración de Presupuesto de TIC:** De acuerdo a los procedimientos de la compañía, anualmente cada líder de área debe presentar con base en los planes para el año siguiente, el presupuesto proyectado, realizando la correspondiente justificación. Es responsabilidad del área realizar el presupuesto anual de TIC, teniendo en cuenta los costos recurrentes de operación y mantenimiento actual y los recursos necesarios para el desarrollo de los nuevos planes de TI.

El área debe formalizar también las prioridades de asignación de recursos y el orden de inversión, maximizando la contribución de TI a las necesidades de la empresa y la oportunidad de la inversión para obtener adecuados resultados.

1.2.4. Procesos de organización de TI

- **Capacitación para el Recurso Humano de TI:** El responsable del área debe identificar las necesidades, oportunidad de formación y promover el entrenamiento continuo del recurso humano de TI, justificar ante la Dirección y velar por la eficacia de los resultados de la capacitación.
- **Gestión de roles, responsabilidades, perfiles del área:** El Director debe determinar las funciones y responsabilidades de cada cargo, asegurándose que los miembros del equipo de trabajo tengan las habilidades, el conocimiento y los recursos necesarios para que éstas se cumplan apropiadamente. También debe velar por que exista un manual de funciones de los cargos. Esta gestión debe buscar apoyo en el área de Recursos Humanos de la compañía.

1.3. Evaluación del estado de tecnologías en la empresa “T”

Con el propósito de evaluar el estado de las tecnologías de información y comunicación en la empresa, el equipo de trabajo definió y aplicó como metodología la construcción de dos matrices estratégicas muy conocidas que permiten obtener una visión global e

integral de la situación y facilitan el análisis de la información recogida. Estas dos matrices son:

- **Matriz de las cuatro acciones:** Permite identificar los elementos de valor de TIC en la organización respondiendo 4 preguntas claves que buscan cuestionar el modelo de tecnología actual:
 - Qué factores se deben reducir?
 - Qué factores deben ser eliminados?
 - Cuáles aspectos se deben incrementar?
 - Cuáles aspectos se deben crear o implementar?

Para desarrollar esta matriz se utilizaron dos mecanismos de recolección de información: 1) A través de la encuesta de estado de TICs realizada a los coordinadores y/o líderes de área y personal de nivel directivo dónde mediante preguntas abiertas se solicitaba contestar estas 4 cuestiones claves; y 2) Mediante una sesión de lluvia de ideas donde participó el equipo de trabajo del Área de Sistemas aportando su percepción sobre estos aspectos basados en la propia experiencia y en la obtenida en la interacción con los usuarios.

- **Matriz DOFA:** Permite enfrentar diversidad de factores internos (fortalezas y debilidades) y externos (oportunidades y amenazas) del área y servicio de TI en la organización, buscando generar alternativas y estrategias para mejorar la gestión de TIC's y la percepción de los clientes internos y externos de la compañía.

El desarrollo de esta matriz requirió participación del equipo de trabajo del área de sistemas así: a cada uno de los miembros del equipo se le solicitó elaborar, desde

su punto de vista y atendiendo a los comentarios recibidos de los usuarios, una lista de las fortalezas y debilidades del área y de las tecnologías de información y comunicación implantadas en la empresa. También se solicitó que teniendo en cuenta el entorno, las nuevas tecnologías, los conocimientos y experiencia de cada uno, se elaborara un listado de las oportunidades y amenazas que observaban podía tener el área en el futuro a corto plazo. Luego, se llevo a cabo una reunión donde se expresaron y sustentaron las ideas de cada uno y por discusión y consenso se definió el listado definitivo de estos 4 factores. Por lluvia de ideas, teniendo en cuenta las opiniones de miembros del equipo y los resultados de la matriz de las 4 acciones realizada previamente, el equipo definió las estrategias que pretende adoptar el área para mejorar su desempeño y así ofrecer un mejor servicio al cliente.

1.3.1. Matriz de las 4 Acciones

<p style="text-align: center;">Eliminar</p> <p>¿Qué factores hoy tenidos en cuenta carecen de valor en la actualidad o incluso nos alejan de aquellos considerados de valor por el cliente?</p>	<p style="text-align: center;">Incrementar</p> <p>¿Qué factores deben ser incrementados por encima de los niveles considerados por la empresa con el objeto de mejorar el servicio?</p>
<ul style="list-style-type: none"> • Paquetes desactualizados de software • Equipos obsoletos de las obras • Uso inadecuado de los sistemas de impresión 	<ul style="list-style-type: none"> • Aprovechamiento de la información administrada en el ERP • Telecomunicaciones y redes inalámbricas • Ingreso fácil y ágil de la información al ERP • Automatización de procesos • Herramientas y reportes para facilitar la toma de decisiones • Herramientas de administración de inventario de hardware y software • Herramienta de control remoto y monitoreo de equipos • Capacidad de los usuarios para emplear herramientas tecnológicas. • Controles sobre el uso de la información • Gestión de requerimientos de mantenimiento en el ERP.
<p style="text-align: center;">Reducir</p> <p>¿Qué factores han sido sobredimensionados como consecuencia de la carrera emprendida para satisfacer necesidades inmediatas de los clientes?</p>	<p style="text-align: center;">Crear</p> <p>¿Qué factores - nunca antes considerados- deben ser creados, buscando descubrir valor para los clientes?</p>
<ul style="list-style-type: none"> • Necesidad de soporte en el ERP • Tiempos de atención de soporte • Reprocesos por errores de configuración 	<ul style="list-style-type: none"> • Mecanismos de consulta de información de los stakeholders a través de Internet • Mecanismos de ingreso de información desde el sitio donde se produce a través de dispositivos móviles • Mecanismos de respaldo de los canales de comunicación de las obras • Capacitación en TIC's • Plan de Contingencia • Listas de chequeo de liberación de equipos de computo

1.3.2. Matriz DOFA (Debilidades – Oportunidades – Fortalezas – Amenazas)

	FORTALEZAS (F)	DEBILIDADES (D)
MATRIZ DOFA	<ol style="list-style-type: none"> 1. Apoyo de la Alta Dirección a la adopción de tecnologías de Información y Comunicación (TICs) 2. Las TICs se encuentran en el Plan Estratégico de la Compañía y se asigna presupuesto al área. 3. Cableado Estructurado Categoría 7 con todos los puntos certificados. 4. Equipos de computo de la Oficina Central 5. Centro de Datos cuenta con condiciones aptas para la necesidad de la compañía. 6. Esquemas de seguridad perimetral físicos. 7. Conocimiento al interior de la compañía del sistema JD Edwards. 8. ERP permite desarrollo interno, y construcción de informes y aplicaciones a la medida. 9. ERP permite procesar información en batch. 10. Esquema de Backup del ERP. 11. Virtualización de algunos servidores del ERP. 12. Soluciones de comunicaciones 13. Vocación de servicio al cliente en el área de Sistemas. 14. Trabajo en Equipo entre áreas y Sistemas. 15. Se cuenta con inventario manual de hardware y software de la compañía. 	<ol style="list-style-type: none"> 1. Usuarios carecen de iniciativa en el uso de TICs. 2. No hay políticas de retención de conocimiento y documentación cuando se generan soluciones a problemas en cualquier componente de TIC's. 3. No hay plan de contingencia de sistemas informáticos establecido, documentado y divulgado. 4. No hay políticas claras en el uso de TICs en la compañía. 5. El Recurso Humano en el área de Sistemas se encuentra reducido, tanto en comparación con el mapa de cargos aprobado, como en relación con el personal total de la compañía, lo que impide soportar la demanda de servicio y genera inconformidad en los usuarios. 6. Deficiencia de equipos de cómputo de puntos remotos. 7. Falla persistente de sistemas de impresión. 8. No hay sistema helpdesk para temas de soporte técnico. 9. La herramienta para que los usuarios generen solicitudes de servicio de soporte y/o mantenimiento del ERP no se está usando, generando desorganización y mala gestión de los requerimientos. 10. Desconocimiento del personal de soporte técnico en algunos temas tecnológicos (Dispositivos Mac, virtualización, etc.) 11. Servidores del ERP son obsoletos y presentan fallas ocasionalmente. 12. Base de Datos del ERP ya no cuenta con soporte y mantenimiento del proveedor. 13. Falta de conocimiento del core del negocio por parte del Partner del ERP. 14. Carencia de sistemas de información no transaccionales. 15. Integración no apropiada del ERP con otros SI. 16. El ERP presenta dificultades en la captura amigable, fácil y ágil de la información. 17. Algunos procesos que se podrían automatizar, aún se ejecutan en el ERP de manera manual.

		<p>18. No se cuenta con mecanismos de consulta de información relevante e interacción de los stakeholders (proveedores, clientes, empleados) a través de Internet.</p> <p>19. Carencia de conectividad inalámbrica en algunos puntos remotos.</p>
OPORTUNIDADES (O)	ESTRATEGIAS FO	ESTRATEGIAS DO
<ol style="list-style-type: none"> 1. Tecnologías de trabajo colaborativo 2. Tercerización de servicios 3. Cloud Computing y Virtualización 4. Aplicaciones en Dispositivos Móviles 5. Equipos de impresión multifuncionales 6. Aplicaciones de Licencia Libre 7. Beneficios ofrecidos por nuevos sistemas como CRM, BI, BPM 8. Cursos, tutoriales y videos on-line sobre herramientas tecnológicas y aplicaciones 9. Masificación de Internet e intercambio de información online. 10. Diversidad de equipos y servicios de internet inalámbrico. 11. Herramientas de trabajo remoto 	<ul style="list-style-type: none"> • Estimular programas de capacitación a través de las herramientas de trabajo colaborativo y las redes LAN. (F12,O1) • Automatizar el inventario de hardware y software de la empresa a través de una herramienta de software libre (F15,O6) • Evaluar los esquemas de cloud computing y virtualización para una futura migración de los sistemas de información (F1,O3) • Desarrollar mecanismos de captura de información a través de dispositivos móviles para facilitar la operación de los usuarios y fortalecer el ingreso en tiempo real de la información. (F7,O4) • Evaluar y licenciar una herramienta de control y monitoreo remoto de equipos. (F12,O11) 	<ul style="list-style-type: none"> • Implementar puntos de impresión y digitalización en la Oficina Principal empleando impresoras multifuncionales. (D7,O5) • Implementar una herramienta de software libre para gestionar el helpdesk que permita también documentar las soluciones. (D2,D8,O6) • Generar espacios para que los integrantes del equipo de Sistemas aprendan de nuevas tecnologías y dispositivos Mac a través de la práctica y apoyados en los cursos y tutoriales ofrecidos en Internet (D10,O8) • Promover la integración de sistemas CRM, BI y BPM que apunten a fortalecer la gestión y consolidación de la información y la toma de decisiones estratégicas en la organización (D14,O7) • Generar herramientas para proporcionar información a las partes interesadas a través del portal corporativo. (D18,O9) • Implementar redes inalámbricas seguras en cada uno de los puntos remotos de la compañía. (D19,O10)
AMENAZAS (A)	ESTRATEGIAS FA	ESTRATEGIAS DA
<ol style="list-style-type: none"> 1. Ataques a vulnerabilidades 2. Obsolescencia y falta de soporte sobre Base de Datos del ERP. 3. Acelerado desarrollo de TIC puede agilizar la obsolescencia de equipos de computo 4. Sobrecosto por temas de mal uso de los equipos de impresión y por cultura de imprimir todo. 5. Fallas Definitivas en Servidores 	<ul style="list-style-type: none"> • Desarrollar un plan de contingencia que permita en caso de fallas en el canal de comunicaciones continuar con la operación en modo off-line, y luego cuando todo se restaure, actualizar el sistema fácilmente. (F7,F9,A6) • Implementar canales alternos de comunicación en los puntos que se requiera y donde la relación costo/beneficio resulte 	<ul style="list-style-type: none"> • Contratar una firma de consultoría especializada en Base de Datos del ERP y garantizar una revisión y mantenimiento periódico de la Base de Datos. (D13,A2) • Repotenciar y mejorar la configuración de los equipos de computo de los puntos remotos. (D6,A3) • Documentar, divulgar y promover un plan de contingencia de sistemas informáticos que garantice la operación, a pesar de caídas en el canal de comunicaciones o fallas eléctricas. (D3,A6)

<p>de ERP.</p> <p>6. Fallas en los canales de comunicación</p> <p>7. Demanda creciente del servicio</p> <p>8. Incremento acelerado del número de usuarios del ERP</p> <p>9. Pérdida de tiempo en reprocesos por mala definición de requerimientos técnicos de las solicitudes de mantenimiento al ERP</p> <p>10. Mal uso y desaprovechamiento de los recursos de TIC de la compañía.</p>	<p>conveniente garantizando conectividad. (F1,A6)</p> <ul style="list-style-type: none"> • Desarrollar mecanismos o puntos de control dentro del sistema de información (ERP), evitando que los controles sean realizados en papel, rompiendo la cultura de imprimir todo. (F8,A4) • Realizar validaciones y pruebas de efectividad de los backups del ERP para garantizar efectividad de las copias en caso de fallas en los servidores. (F10,A5) • Contratar un servicio o probar herramientas de monitoreo de la red y de detección de vulnerabilidades para proteger la infraestructura y la red de ataques. (F3,F5,A1) • Aumentar capacidad de los servidores de ERP para garantizar respuesta óptima a los usuarios. (F11,A8) 	<ul style="list-style-type: none"> • Contratar un Ingeniero más para el Departamento de Sistemas para permitir distribuir la carga laboral y mejorar los indicadores de servicio. (D6,A6) • Generar un relanzamiento de la herramienta para ingresar requerimientos de mantenimiento del ERP, que permita que el usuario documente su necesidad, y participe en la construcción de la solución, minimizando reprocesos. (D10,A8) • Desarrollar una campaña para promover el buen uso de los equipos de impresión y evitar la impresión innecesaria. (D8,O4) • Implementar la renta de equipos de cómputo como mecanismo que permite renovación tecnológica y actualización frecuente, evitando costos de depreciación (D7,A3) • Elaborar, divulgar y oficializar las políticas de TIC de la compañía. (D4,A10)
--	---	---

1.3.3. Análisis y Priorización de Estrategias

Las estrategias definidas en la matriz DOFA están agrupadas para alcanzar 4 propósitos definidos en orden de prioridad así:

- 1) Mejoramiento del desempeño de los servicios asociados al ERP: Este es un punto neurálgico de la operación de la compañía, por lo que requiere el mayor esfuerzo. Este es un servicio que no puede fallar; no es una gran oportunidad de mejora, sino un requisito de servicio. Teniendo en cuenta que todos los componentes de la infraestructura asociada al ERP (hardware de servidores, software de servidores, sistema ERP y motor de base de datos) están perdiendo soporte, este aspecto es sumamente sensible y requiere la mayor prioridad. Tal vez no es posible una mejora sustancial de la infraestructura, pero es necesario mantenerla lo mejor posible.
- 2) Soporte de la gestión del área con herramientas de software: El equipo de trabajo del área de Sistemas es insuficiente, y teniendo en cuenta el crecimiento de la empresa, el trabajo se ha multiplicado, por lo que la implementación de herramientas informáticas como sistema de helpdesk, soporte remoto, inventario de hardware y software es necesaria para optimizar tiempos y aprovechar los recursos. De igual manera, es importante detectar y corregir el origen de muchas de las fallas que ocasionan llamadas de soporte que demandan tiempo del personal del área, entre estas, los problemas de impresión y la obsolescencia de algunos equipos de computo.
- 3) Promover metodologías y políticas para mejoramiento de la gestión de TI. El análisis permite identificar que la operación de la compañía está apoyada en gran medida por las tecnologías de información y comunicación, lo que hace necesario implementar controles y metodologías de mejoramiento sobre ésta infraestructura.

- 4) Adopción de nuevas tendencias informáticas y uso de tecnologías para mejorar la experiencia de las partes interesadas: El análisis de las matrices y de la evaluación de madurez demuestra que la organización encuentra en el uso de las Tecnologías de información y comunicación un factor para apoyar el logro de las estrategias corporativas y que la Alta Gerencia, consciente de las bondades de estas, ha realizado fuertes inversiones en la plataforma tecnológica. Sin embargo, los avances de las herramientas y sistemas informáticos generan nuevas necesidades en los usuarios internos y externos: los empleados necesitan contar con mejores y más útiles herramientas para desarrollar su trabajo, los directivos y socios requieren información oportuna y clave para facilitar la toma de decisiones, los clientes demandan servicios flexibles, posibilidad de realizar transacciones y acceder a toda la información de su interés de manera simple, las entidades gubernamentales generan exigencias que se cumplen más fácilmente con la adopción de tecnologías. Todo lo anterior demuestra que es indispensable evolucionar con cierta frecuencia, y con mayor razón cuando se quiere lograr ventaja competitiva.

1.4. Identificación de necesidades de TI en la empresa “T”

El análisis realizado a lo largo del capítulo permite enunciar las siguientes necesidades de TI detectadas al interior de la organización:

- Es necesario adicionar por lo menos un Ingeniero al equipo de trabajo del Departamento de Sistemas para permitir distribuir la carga laboral y mejorar los indicadores de servicio.
- Generar espacios para que los integrantes del equipo de Sistemas aprendan de nuevas tecnologías y dispositivos Mac.
- Es conveniente definir mecanismos para garantizar el respaldo del recurso humano en caso de ausencia de cualquier miembro del equipo.

- Se requiere enfocar esfuerzos en el desarrollo de procesos de planeación y organización del área de TI que incluyan: elaboración de plan estratégico de TIC, control presupuestal, definición de políticas y procedimientos del área, estructura del área, planeación de capacitación, establecimiento de indicadores de gestión y evaluación de desempeño del área. También se debe elaborar, divulgar y oficializar las políticas de TIC de la compañía.
- Es indispensable desarrollar, probar, documentar, divulgar y mantener un Plan de contingencia de TIC que permita continuar la operación en caso de fallas.
- Es necesario generar una política clara de soporte y mantenimiento controlando los requerimientos sobre el sistema de información (ERP). Se debe establecer un estándar para solicitud y recepción de requerimientos, contar con un proceso definido de levantamiento, recepción, documentación, aceptación, entrega y control de cambios, y definir un proceso para la planeación, ejecución y monitoreo de los proyectos de desarrollo de software.
- Se requiere la implementación de una herramienta de helpdesk que permita el registro, control y documentación del soporte técnico ofrecido.
- Se requiere la implementación de una herramienta sistematizada para controlar el inventario de Hardware y Software de la compañía.
- Es necesario evaluar y licenciar una herramienta de control y monitoreo remoto de equipos.
- Se requiere el desarrollo de mecanismos de captura de información a través de dispositivos móviles para facilitar la operación de los usuarios y fortalecer el ingreso en tiempo real de la información.

- Es importante generar herramientas para proporcionar información a las partes interesadas a través del portal corporativo.
- Es necesario promover la integración de sistemas CRM, BI y BPM que apunten a fortalecer la gestión y consolidación de la información y la toma de decisiones estratégicas en la organización.
- Se hace relevante cambiar el esquema de servicios de impresión, digitalización y fotocopiado y desarrollar una campaña para promover el buen uso de los recursos, evitando la impresión innecesaria.
- Es necesario repotenciar y mejorar la configuración de los equipos de cómputo de la compañía, lo que se puede lograr implementando la renta de equipos de cómputo como mecanismo que permite renovación tecnológica y actualización frecuente, evitando costos de depreciación.
- Se debe sacar más provecho a la infraestructura tecnológica actual fomentando los programas de capacitación a través de las herramientas de trabajo colaborativo y las redes LAN.
- Es indispensable pensar en el futuro e ir evaluando los esquemas de cloud computing y virtualización para una futura migración de los sistemas de información.
- Resulta conveniente implementar redes inalámbricas seguras en cada uno de los puntos remotos de la compañía y canales alternos de comunicación en los puntos donde la relación costo/beneficio resulte conveniente garantizando conectividad en caso de fallas del canal primario.

- Desarrollar mecanismos o puntos de control dentro del sistema de información (ERP), evitando que los controles sean realizados en papel, rompiendo la cultura de imprimir todo.

- Realizar un monitoreo de la red, detectar y corregir vulnerabilidades para proteger la infraestructura y la red de ataques.

- Tomar medidas para mantener los componentes del sistema ERP y/o minimizar el impacto que ocasiona una falla. Algunas medidas pueden ser: contratar una firma de consultoría especializada en Base de Datos del ERP y garantizar una revisión y mantenimiento periódico de la Base de Datos, realizar validaciones y pruebas de efectividad de los backups del ERP para garantizar efectividad de las copias en caso de fallas en los servidores.

CAPITULO 2

2. IDENTIFICACIÓN DE PROCESOS Y METODOLOGÍAS DE TICS NECESARIOS PARA LA MEJORA

De acuerdo a la evaluación de madurez realizada en la organización se ha logrado detectar que no se cuenta con el desarrollo de las labores de TI, siguiendo alguna metodología o una guía de buenas prácticas tales como ITIL, COBIT, CMMI, ISO 27002. En realidad, el trabajo se realiza y se cumplen los requerimientos, pero no se observa planeación y organización tendiente a la mejora continua.

La adopción de metodologías y de recomendaciones sugeridas por las buenas prácticas de TI puede ayudar a gestionar adecuadamente el Departamento de Sistemas y en general, permitir que la compañía “T” aproveche mejor las tecnologías de información y comunicaciones para apoyar el logro de sus objetivos estratégicos.

2.1. Prácticas recomendadas para la mejora de los procesos actuales

2.1.1. Procesos de Gestión de los Sistemas de Información

Dentro de las mejores prácticas sugeridas en las metodologías CMMI e ITIL, se pueden implementar las siguientes:

- Help Desk (mesa de ayuda): esta herramienta se convierte en el primer punto de contacto entre los usuarios y TI, para la solicitud de requerimientos y soportes, atender inquietudes y resolver inconvenientes de los usuarios.

Para mejorar los procesos de gestión de los sistemas de información, la mesa de ayuda debe recibir los requerimientos de cambios solicitados por los usuarios

en un formato preestablecido, y los canaliza al área directamente encargada. Este primer filtro facilita la depuración de solicitudes y agiliza el análisis de las mismas, suprimiendo los reprocesos que se presentan cuando estas se dirigen a áreas diferentes de la responsable de los desarrollos, y de manera informal. A través del número de tiquete que se asigna al usuario cuando se abre el caso, la persona o área encargada entrega mediante el software que apoya la mesa de ayuda, el estado de la solicitud y la fecha pactada de entrega. Esto refuerza el compromiso con las fecha de liberación de los desarrolladores, y además permite al usuario final planear sus actividades por el conocimiento de los tiempos de entrega.

- CMMI: tomando como marco de referencia esta metodología, se sugiere la adopción de varias áreas de proceso, enfocadas a la gestión de requerimientos, la calidad del software y el mejoramiento continuo.

A continuación se relacionan algunas áreas de proceso, que se sugieren sea implementadas para las cuales se desarrollan los formatos mencionados como anexos como un primer paso de implementación.

Área de proceso	Justificación	Formatos
REQM (Gestión de requerimientos)	Al contar con un proceso de requerimientos definido y un proceso de recepción de requerimientos y controles de cambios se organiza el proceso y se acaba el caos de solicitudes de último momento.	Formato documento de requerimientos (Ver Anexo 2).
PP (Planificación de proyecto)	Ayuda a tener una planeación coherente del trabajo del área de desarrollo y disminuir la carga laboral por sobre-esfuerzo debido a un mal plan o no planeación.	Formato documento de planeación (Anexo 3)
CM (Gestión de la configuración)	Teniendo un proceso estructurado de gestión de la configuración se optimizan tiempos por retrabajos, se tiene control sobre las versiones y artefactos de trabajo.	Formato gestión de cambios (Anexo 4)
VER (Verificación)	Teniendo un proceso de verificación y validación sobre los entregables a liberar se disminuye los errores inyectados en producción.	Formato documento de verificación (Anexo 5)
OT (Formación organizativa)	Esta área apoya el mejoramiento continuo y control a las capacitaciones.	Formato documento de capacitación (Anexo 6)

2.1.2. Procesos de Gestión de Infraestructura de TI

➤ Gestión de acuerdos con proveedores. En CMMI se encuentra un área de proceso enfocada a la relación con los proveedores, que puede usarse como modelo de adopción para la compañía. SAM (Supplier Agreement Management) - Gestión de acuerdos con proveedores, tiene como propósito gestionar la adquisición de productos y servicios de proveedores. En esta se recomienda tres pasos básicos:

- Determinar el tipo de adquisición: los requerimientos del producto, características, presupuesto, garantía, escalabilidad, respaldo del fabricante, etc. Se realiza una investigación sobre las opciones que tiene el mercado y como estas pueden cubrir las necesidades de TI.
- Selección de proveedores: a través de una herramienta como una matriz de calificación de proveedores, se evalúan por lo menos dos o tres opciones, teniendo como ítems de evaluación la experiencia en el campo, el músculo financiero, referencias, servicio postventa, representación local, opciones de pago y valor de cotización. Estos puntos se ponderan de acuerdo a la importancia de cada uno para la negociación en particular y se selecciona la mejor opción.
- Establecer acuerdos con el proveedor: se formaliza la relación mediante contratos, licencias o similares, donde el proveedor debe incluir una declaración de las actividades, especificaciones, los términos y condiciones, una lista de entregables, un calendario, la definición de los SLA (acuerdos de nivel del servicio), un presupuesto y un proceso de aceptación definido.

Una vez cumplidas estas etapas iniciales, se desarrollan las actividades o la entrega y puesta en funcionamiento del producto adquirido, conforme a los

acuerdos suscritos con el proveedor. Estos deben monitorearse para controlar el cumplimiento de los tiempos y el progreso general de la implementación.

Se desarrollan los siguientes formatos con el fin de establecer el una primera aproximación de la implementación de esta área de proceso.

Formato acta de reunión (Anexo 7)

Formato - adquisición hardware – software (Anexo 8)

- Fase Diseño del servicio de ITIL: en esta etapa del ciclo de vida de ITIL, se diseñan y desarrollan los servicios, tanto nuevos como modificados, buscando satisfacer las necesidades presentes y futuras del negocio, minimizando los riesgos, enfocándose en obtener mayor calidad y en lo posible ahorrando tiempo y dinero. De las practicas de esta fase, se recomiendan las siguientes:
 - Gestión de la capacidad: se encarga que todos los servicios TI se vean respaldados por una capacidad de proceso y almacenamiento suficiente y correctamente dimensionada, que evite el desaprovechamiento de los recursos, las inversiones innecesarias o que los medios sean insuficientes y se degrade la calidad del servicio. Para realizar esto, se debe considerar:
 - Conocer el estado actual de la tecnología, tanto hardware como software (inventario, Ítems de configuraciones, garantías, estado legal, etc).
 - Analizar el rendimiento de la infraestructura para monitorear el uso de la capacidad existente.

- Dimensionar adecuadamente los servicios y aplicaciones alineándolos a los procesos de negocio y necesidades de los usuarios.
- racionalizar el uso de servicios informáticos según la demanda.
- Gestión de la disponibilidad: es responsable de optimizar y monitorear los servicios TI para que estos funcionen ininterrumpidamente y de manera fiable, cumpliendo con entregar un servicio a satisfacción para el cliente, y conservando un nivel de costos razonables. Las actividades sugeridas para la administración de la infraestructura de TI son:
 - Determinar los requisitos de disponibilidad reales del negocio.
 - Mantener el servicio en operación y recuperación en caso de fallo.
 - Realizar diagnósticos periódicos sobre la disponibilidad de los sistemas y servicios.
 - Evaluar el impacto de las políticas de seguridad en la disponibilidad.
 - Evaluar el posible impacto de un cambio en la disponibilidad.
- Fase Transición de servicio de ITIL: es la encargada de garantizar el éxito cuando los servicios nuevos a modificados, pasan de la etapa de diseño a la puesta en producción. La practica que se recomienda esta incluida en la transición del servicio, pero es recurrente en todas las demás fases del ciclo de vida.
 - Gestión de la configuración: no se puede gestionar correctamente lo que se desconoce. Es muy importante conocer en detalle toda la infraestructura TI de la organización, para obtener el mayor provecho de la misma. La principal

tarea de la Gestión de la Configuración es llevar un registro actualizado de todos los elementos de configuración de la infraestructura TI, junto con sus interrelaciones. Para esto, la principal tarea es utilizar y mantener la CMDB (base de datos de la gestión de configuración), donde se registra cada elemento o ítem de configuración, el hardware, el software, la documentación, los cambios y en general los datos pertinentes al servicio de TI.

Las tareas para el control de todos los recursos de la infraestructura de TI, deben centrarse en:

- Asegurar que todos los componentes están registrados en la CMDB.
- Monitorear el estado de todos los componentes.
- Actualizar las interrelaciones entre los ítems de configuración.
- Informar sobre el estado de las licencias.

Administración de la Seguridad Informática

➤ Fase Diseño del servicio:

- Gestión de la seguridad informática: la información es el activo más importante del negocio y su gestión debe apoyarse en tres principios:
 - Confidencialidad: accesible solo a sus destinatarios predeterminados.
 - Integridad: la información debe ser correcta y completa.

- Disponibilidad: fácil acceso a la información cuando se necesita.

La Gestión de la Seguridad debe, por tanto, velar por que la información sea correcta y completa, esté siempre a disposición del negocio y sea utilizada sólo por aquellos que tienen autorización para hacerlo.

Los principales objetivos de la Gestión de la Seguridad son:

- Diseñar una política de seguridad, correctamente alineada con las necesidades del negocio.
- Asegurar el cumplimiento de los estándares de seguridad acordados.
- Minimizar los riesgos de seguridad que amenacen la continuidad del servicio.

Es necesario evaluar rigurosamente el proceso para asegurar que la Gestión de la Seguridad cumple sus objetivos, que se verán reflejados en la disminución de incidentes que atenten contra la seguridad, acceso eficiente a la información por parte de las personas autorizadas y la identificación de manera proactiva de vulnerabilidades y amenazas que pueden degradar la calidad del servicio.

2.1.3. Procesos de planeación de TI

Siguiendo las buenas prácticas, la empresa puede implementar lo siguiente:

- **Aseguramiento de la Calidad:** Se debe velar por implementar mecanismos o controles que permitan garantizar que los desarrollos de software se liberan a

producción, solo cuando se ha validado completa y correctamente su desempeño y que se ajusta a los requerimientos del cliente interno de la compañía.

También se debe realizar una evaluación periódica del desempeño de la infraestructura, evitando fallas.

- **Elaborar Plan estratégico de TIC:** El área debe gestionar y dirigir los recursos de TI de acuerdo a los objetivos estratégicos de la compañía. Debe evaluar periódicamente si la plataforma tecnológica existente está satisfaciendo las necesidades del negocio y si contribuyen adecuadamente con el logro de esos objetivos.

Conforme la Alta Dirección define una planeación estratégica de la organización, el área de TI debe realizar una planeación estratégica de TIC que permita apoyar la consecución de las metas organizacionales.

También es responsabilidad del área monitorear las tendencias tecnológicas emergentes y las tendencias y regulaciones que van surgiendo en el sector con el propósito de preparar y /o adaptar la infraestructura de TI de la empresa.

A nivel táctico, se debe establecer el plan para lograr la gestión y monitoreo de los recursos de TI.

- **Control de Ejecución de Presupuesto:** Es conveniente implementar acciones para controlar periódicamente la ejecución del presupuesto, logrando identificar el estado de inversión Vs. el logro de los objetivos propuestos en el plan de inversión del presupuesto inicial.

Es conveniente también ir comparando los costos reales frente a los costos presupuestados

- **Evaluar madurez informática de la empresa:** Con el propósito de identificar las motivaciones del uso de tecnología en la organización y buscar alinear la tecnología con las metas estratégicas de la compañía es conveniente analizar el estado de madurez informática de la compañía. Esto implica identificar las tecnologías de información y comunicación usadas, el grado de aceptación y participación que los usuarios tienen con la tecnología, el estado de procedimientos y metodologías en el área de TI, y en general todos los aspectos que permitan posicionar la empresa teniendo en cuenta algún modelo de evaluación de madurez en TI.

- **Evaluar coherencia entre Estrategia de Negocio y Estrategia de TI:** Siempre será conveniente validar que la estrategia de TI apoye la estrategia de negocio de la compañía, porque es probable que las acciones emprendidas en cada una, apunten a objetivos, que aunque se realizan en beneficio de la organización, no estén sirviendo para sumar esfuerzos y apuntar a una meta común.

2.1.4. Procesos de organización de TI

- **Estructurar y organizar el área:** Es responsabilidad del Director del área definir la estructura interna del área, establecer la misión, las metas del área y los planes para alcanzarlas.

- **Definir políticas y procedimientos de TI:** Incluye:
 - Promover la captura y difusión del conocimiento a través de la documentación y de programas de entrenamiento entre miembros del equipo.

- Definir política de respaldo del personal de TI
 - Definir políticas de manejo y confidencialidad de la información de la compañía
 - Definir procedimientos a seguir en caso de contingencias
 - Definir procedimientos para gestión de usuarios.
- **Planeación de capacitación del Recurso Humano de TI:** El Director del área debe identificar y diseñar un programa de capacitación y entrenamiento del recurso humano de TI. Es posible planear que la capacitación sea recibida por algún miembro del equipo, y se utilicen estrategias de replicación de lo aprendido a los demás integrantes del área.

Se deben establecer el alcance, los objetivos y participantes de la capacitación, elegir si se desea realizar capacitación interna o externa, presupuestar el costo, y planear oportunamente para evitar conflictos con períodos de alta carga laboral.

- **Establecer indicadores de gestión y evaluar desempeño:** No es posible evaluar lo que no se mide, por lo que será necesario plantear y formalizar indicadores que permitan conocer el desempeño del área, el nivel de soporte ofrecido, el número de horas empleadas para brindar una solución, el ranking de problemas frecuentes. Solo midiendo el desempeño se obtienen herramientas para tomar decisiones y fomentar acciones para fortalecer el servicio del área.
- **Desarrollar Plan de contingencia:** El área de TI debe definir, documentar y divulgar un plan de contingencia que permita retomar la operación en el menor

tiempo posible, al presentarse algún incidente o situación que afecte la plataforma tecnológica de la compañía.

Controlar y actualizar planes de contingencia de TIC: El plan de contingencia implementado debe revisarse periódicamente para analizar si se ajusta a las necesidades actuales de la organización. En caso de ser requerido, debe actualizarse y divulgar las actualizaciones.

CAPITULO 3

3. PLAN DE CONTINGENCIA DE TI PARA EL SISTEMA DE INFORMACIÓN CORPORATIVO

3.1. Alcance

El presente plan de contingencia pretende indicar los procedimientos a seguir en caso de falla en cualquier componente de la plataforma tecnológica que soporta el sistema de información actual de la compañía, es decir, el ERP J.D. Edwards.

Los procedimientos específicos, en caso de contingencia, de cada una de las áreas de la compañía que gestionan su información en el ERP, serán elaborados y documentados por cada líder de área y junto con este Plan de Contingencia de TI, conformarán el Plan de Contingencia Integral de la Organización.

3.2. Objetivo general

Garantizar que los procesos críticos de operación de la compañía puedan continuar desarrollándose, a pesar de no contar con la disponibilidad del sistema de información.

3.3. Objetivos específicos

- Establecer el procedimiento que debe seguir el equipo del Departamento de Sistemas para entregar a los usuarios respaldo durante y después del incidente presentado en la plataforma informática del ERP.
- Definir los mecanismos para almacenar la información clave que debe registrarse, así sea de manera manual, continuando con el desarrollo de los procesos críticos de la compañía.

- Definir las prácticas ideales para disminuir los tiempos que requiera la puesta en marcha del plan de contingencia durante la presentación de un incidente.

3.4. Descripción del servicio

El ERP es el sistema de información en el que se registra toda la operación financiera, contable, de compras e inventarios, y ventas de la compañía.

Los servidores que proporcionan el sistema de información son cuatro y se encuentran en un Data Center fuera de las instalaciones de la compañía, administrados por un tercero con quien se tiene contratado el servicio de hosting y colocation por outsourcing. Todas las actividades necesarias para velar por la seguridad física y lógica de estos servidores y la administración del sistema operativo son responsabilidad del proveedor, de acuerdo al contrato realizado entre las partes.

El outsourcing debe garantizar backups e imágenes espejo de los servidores y de las bases de datos contenidas en estos con periodicidad diaria, semanal y mensual de acuerdo con los requerimientos establecidos por la compañía. Los backups diarios se almacenan en disco externo y los backups semanales y mensuales se almacenan en discos externos y en cintas que tienen políticas de retención y que se guardan en sitio seguro.

El outsourcing también debe garantizar un nivel de servicio del 99.7% en la disponibilidad del canal de comunicaciones.

En caso de fallas con algún componente físico de los servidores, el proveedor proporciona un servicio bajo demanda de replica del servidor en otro rentado. Se cuenta con herramientas de monitoreo que permitan prever fallas en algún componente de la plataforma.

Ahora bien, la información, las aplicaciones y el sistema de información contenido en los servidores son responsabilidad del Departamento de Sistemas de la compañía. Las bases de datos se encuentran en DB2 y la administración básica es propia; sin embargo, se cuenta con un proveedor de consultoría especializado en este motor de Base de Datos.

Teniendo en cuenta que los servidores no se encuentran en las instalaciones de la compañía, se requiere el uso de redes WAN para acceder al sistema. Para el ambiente Web se hace uso de la red de Internet, y para el ambiente Terminal se hace uso de un canal dedicado contratado con un ISP. Los servidores son:

- **Servidor Terminal:** dedicado a ofrecer el acceso por escritorio remoto. Este servidor se encuentra virtualizado y cuenta con un sistema operativo Windows 2000 Advanced Server.
- **Servidor Empresarial:** es el servidor que aloja las bases de datos y los servicios de operación del sistema. Este servidor ya no cuenta con garantía y tiene un sistema operativo Windows 2000 Advanced Server.
- **Servidor Despliegue:** Permite el desarrollo y despliegue de software. Este servidor ya no cuenta con garantía y cuenta con un sistema operativo Windows 2000.
- **Servidor Web:** dedicado a ofrecer acceso por ambiente web. Este servidor ya no cuenta con garantía y tiene un sistema operativo Windows 2003 Server Standard Edition.

El acceso al sistema se puede realizar de dos maneras: por ambiente Terminal mediante conexión por escritorio remoto y por ambiente Web a través del acceso a una página de Internet.

En la actualidad, todos los usuarios de la Oficina principal, salas de ventas y obras ingresan por ambiente terminal; sin embargo, el ambiente web está disponible como contingencia.

Para ingresar al servidor terminal, solo es posible hacerlo desde la IP pública fija de la compañía, debidamente identificada y aceptada por el firewall del centro de datos donde están alojados los servidores.

Todos los puntos externos a la Oficina Principal, cuentan con canales ADSL y dedicados que son administrados de manera tal que al realizar peticiones de conectividad hacia el servidor terminal, este tráfico se enruta hacia un equipo de red o router ubicado en la oficina principal, y desde allí se enruta finalmente hacia el servidor terminal tomando como IP origen la IP pública de la compañía, que es la única IP autorizada para acceder al servidor terminal.

La gestión de los canales de comunicaciones y equipos que se encuentran en el Data Center interno de la compañía y que sirven de enrutador hacia el servidor Terminal del Data Center externo, es responsabilidad del Departamento de Sistemas de la compañía.

3.5. Análisis y valoración de riesgos

- Riesgos sobre los servicios de Red**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> Inestabilidad del Sistema Operativo Bloqueos sobre los servicios por parte de componentes de seguridad de Red. Permisos del usuario ejecutor de los servicios sobre el Sistema Operativo. 	<p>Grado de Impacto: Alto</p> <p>Probabilidad de ocurrencia: Baja</p>	<ul style="list-style-type: none"> Establecer una lista con cada uno de los servicios que intervienen en el proceso. Detallar las tareas realizadas por cada servicio Clasificar los servicios según el componente de software que afecta. Detallar los permisos de ejecución requeridos sobre el Sistema Operativo. 	<ul style="list-style-type: none"> Verificar el proceso afectado. Verificar en la lista de servicios y sus detalles, cuales son los posibles servicios que afectan el proceso. Verificar el estado y ejecución (ocurre que los servicios se encuentran activos, pero no se están ejecutando). Identificar los servicios afectados. Tomar las medidas correspondientes y reiniciar los servicios afectados. 	<ul style="list-style-type: none"> Ing. Desarrollo

- Riesgos sobre los Sistemas Operativos (S.O.)**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> Desactualización del S.O. Amenazas de seguridad como virus y ataques informáticos. Perdida de soporte por parte del proveedor sobre la 	<p>Grado de Impacto: Alto</p> <p>Probabilidad de</p>	<ul style="list-style-type: none"> Mantener actualizado el S.O. Siempre verificar los conflictos que puede tener un release del Sistema Operativo antes de instalarlo. Mantener el Sistema Operativo con un 	<ul style="list-style-type: none"> Verificar el log de eventos. Identificar el error. Verificar el origen del error. Si el error presentado es desconocido, o por conflictos, se debe verificar las últimas actualizaciones realizadas, o verificar si el proveedor cuenta con un 	<ul style="list-style-type: none"> Ing. Desarrollo Outsourcing

<p>versión instalada.</p> <ul style="list-style-type: none"> • Conflictos de ejecución con aplicaciones instaladas. • Omisión de los requerimientos de hardware especificados por parte del proveedor. • Malas acciones administrativas sobre el S.O. 	<p>ocurrencia: Alta</p>	<p>sistema de seguridad que incluya aparatos de red y sistema antivirus.</p> <ul style="list-style-type: none"> • Registrar los eventos del S.O. en un log de eventos, con el fin de determinar el origen de los fallos. • Restringir el acceso con privilegios administrativos al servidor. • Mantener una copia de respaldo del servidor. • Realizar labores administrativas con el fin de mantener el S.O. en óptimas condiciones. 	<p>nuevo release del S.O., que solucione el bug.</p> <ul style="list-style-type: none"> • Realizar labores administrativas sobre el S.O. Acciones como limpieza de logs, evaluación de servicios, verificación de niveles de procesamiento en la CPU y consumo de memoria. • Reportar el problema con el proveedor. 	
--	-------------------------	---	---	--

• **Riesgos sobre las Bases de Datos (BD)**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> • Desactualización del motor de Base de Datos. • Pérdida de soporte por parte del proveedor. • Ejecución de procesos automáticos y/o programados que afecten el desempeño de la BD. • Incumplimiento de requerimientos mínimos de 	<p>Grado de Impacto: Muy Alto</p> <p>Probabilidad de ocurrencia: Media</p>	<ul style="list-style-type: none"> • Establecer y ejecutar un plan de mantenimiento preventivo sobre la Base de Datos. • Verificar, el impacto de cada uno de los cambios de software que puedan comprometer el comportamiento de la Base de Datos, del Sistema Operativo o el manejo de recursos. • Establecer una lista de chequeo con los requerimientos que debe cumplir cada proceso 	<ul style="list-style-type: none"> • Verificar el log del motor, con el fin de identificar el origen del problema. • Verificar consumos excesivos o conflictivos sobre el motor de Base de Datos con herramientas administrativas de DB2. • Verificar a nivel de Sistema Operativo posibles conflictos generados. • Verificar nuevos release con el fin de verificar si son problemas resueltos mediante actualización. 	<ul style="list-style-type: none"> • Ingeniero de Desarrollo

<p>software y hardware.</p> <ul style="list-style-type: none"> • Acciones administrativas erróneas que generen un mal uso de los recursos. • Ejecuciones transaccionales, que dejen procesos abiertos al finalizar la ejecución. • Incompatibilidad entre el motor de BD, el S.O. y las aplicaciones instaladas. 		<p>automático que se ejecutará sobre el motor.</p> <ul style="list-style-type: none"> • Validar el impacto sobre los recursos del servidor de cada nueva ejecución a realizar sobre el motor. • Restringir el acceso al motor de Base de Datos. • Establecer un plan de backup para los contenidos de la Base de Datos. 	<ul style="list-style-type: none"> • Si el daño es irreparable, es necesario realizar una restauración del último backup. • Se deberá contactar al consultor de la Base de Datos, en caso de requerirse asesoría. 	
---	--	--	---	--

• **Riesgos sobre aplicaciones de apoyo a ERP (Visor de PDF)**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> • Daños sobre la instalación del software. • Procesos ejecutados paralelamente, que detengan la ejecución del software. • Actualización mal instalada. 	<p>Grado de Impacto: Bajo</p> <p>Probabilidad de ocurrencia: Baja</p>	<ul style="list-style-type: none"> • Verificar incompatibilidades antes de instalar actualizaciones. • Mantener actualizado el software. 	<ul style="list-style-type: none"> • Verificación del estado de los servicios ligados al software. • Reinicio de los servicios. • Reinstalación del software. 	<ul style="list-style-type: none"> • Ingeniero de Desarrollo • Outsourcing

- **Riesgos sobre aplicaciones de apoyo a ERP (Office Word, Excel)**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> • Actualizaciones incompatibles. • Bugs generados por actualizaciones del S.O. • Mal funcionamiento de los servicios, por consumo excesivo. 	<p>Grado de Impacto: Medio</p> <p>Probabilidad de ocurrencia: Baja</p>	<ul style="list-style-type: none"> • Mantener actualizado Office. • Evaluar las actualizaciones de seguridad antes de instalarlas. 	<ul style="list-style-type: none"> • Reconocimiento de los servicios. • Verificar si el problema presentado se soluciona con un release del proveedor. • Reinstalar el software. 	<ul style="list-style-type: none"> • Ingeniero de Soporte • Outsourcing

- **Riesgos de caída del canal de comunicaciones hacia el Data Center Externo**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> • Perdida de sincronización entre los equipos del proveedor de comunicaciones. • Daño en los medios físicos (fibra óptica, cobre). 	<p>Grado de Impacto: Muy Alto</p> <p>Probabilidad de ocurrencia: Baja</p>	<ul style="list-style-type: none"> • Definir unos acuerdos de nivel de servicio estrictos con el proveedor de comunicación. 	<ul style="list-style-type: none"> • Revisar la traza de los paquetes para determinar dónde se cae la conectividad. • Solicitar ingreso a los usuarios por ambiente Web. • Contactar inmediatamente al proveedor de comunicación. • Hacer cumplir los SLA's. 	<ul style="list-style-type: none"> • Ingeniero de Soporte • Outsourcing

- **Riesgo caída canal de comunicaciones entre los puntos remotos y la Oficina Principal**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> • Fallas en el servicio ADSL del punto remoto. • Falla en el equipo de conectividad Rhino Box. • Daño físico en las líneas telefónicas. 	<p>Grado de Impacto: Alto</p> <p>Probabilidad de ocurrencia: Alto</p>	<ul style="list-style-type: none"> • Permitir en el firewall el acceso del tráfico proveniente de cada una de las direcciones IP de los canales ADSL de los puntos remotos, usadas como segunda alternativa de conectividad. 	<ul style="list-style-type: none"> • Contactar inmediatamente al proveedor de servicio de internet. • Realizar recarga en los dispositivos modem USB. Si el punto remoto cuenta con router inalámbrico USB, y si la falla no se presenta en el Rhino Box, este automáticamente detecta el problema en la interface del ISP y enruta el tráfico por el modem USB. Si el punto remoto no cuenta con router, se conectará el modem USB a un solo equipo en el que se deberán realizar las actividades más urgentes. • Si la falla es en el Rhino Box, se debe restaurar sobre este el último backup. 	<ul style="list-style-type: none"> • Ingeniero de Soporte

- **Riesgo de fallas en los equipos de Red**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> • Daño en los componentes electrónicos por deterioro. • Puertos quemados por filtración de energía en el cableado de datos o 	<p>Grado de Impacto: Muy Alto</p>	<ul style="list-style-type: none"> • Backup actualizado del firmware y la configuración. • Documentar la configuración: claves, direcciones, rutas, accesos, etc. • Contar en la Oficina 	<ul style="list-style-type: none"> • Si la falla es en un switch y el punto remoto cuenta con otros, dar las indicaciones al personal en sitio sobre cómo instalar y conectar el dispositivo. • Contar con un software de control de intrusos que 	<ul style="list-style-type: none"> • Ingeniero de Soporte

<ul style="list-style-type: none"> • picos de voltaje. • Falla por ataque interno o externo. 	<p>Probabilidad de ocurrencia: Media</p>	<p>Central con las fotografías de la configuración de la red y los equipos, de manera que se pueda dar instrucciones y guiar de manera precisa a los funcionarios en sitio sobre cómo reiniciar, conectar o mover los equipos.</p> <ul style="list-style-type: none"> • Diagramar el mapa de red con la función de los equipos. 	<p>permita bloquearlos y localizarlos.</p> <ul style="list-style-type: none"> • Denunciar ante las autoridades competentes los ciberataques. 	
--	--	--	---	--

• Riesgo de Fallas en el Router Rhino Box de la Oficina Principal

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> • Daño en componentes de hardware. • Daño en el sistema operativo. • Falla por ataque interno o externo. 	<p>Grado de Impacto: Muy Alto</p> <p>Probabilidad de ocurrencia: Baja</p>	<ul style="list-style-type: none"> • Backup actualizado del software y la configuración: seguridades, perfiles, aplicaciones y reglas. • Stock de refracciones: tarjeta de red, disco duro, memoria y fuente de poder. • Documentación actualizada de las funciones y el uso del equipo. 	<ul style="list-style-type: none"> • Diagnosticar qué componente de hardware fallo, y proceder a su reemplazo. • Si la falla es grave, solicitar al proveedor de Rhino un dispositivo en renta temporal mientras se recupera el equipo propio. Restaurar en el dispositivo rentado el último backup. • Minimizar los permisos en el firewall, para impedir la entrada o salida de paquetes de datos no autorizados, mientras se estabiliza la seguridad. 	<ul style="list-style-type: none"> • Ingeniero de Soporte

- **Riesgo de fallas en los servidores**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> • Daño en componentes de hardware. • Daño en el sistema operativo y/o la configuración. • Daño en el software de producción. • Falta de mantenimiento preventivo. 	<p>Grado de Impacto: Muy Alto</p> <p>Probabilidad de ocurrencia: Baja</p>	<ul style="list-style-type: none"> • Ante la obsolescencia de 3 de los servidores que no tienen garantía, se debe mantener estricto control, revisión y mantenimiento periódico. El cuarto servidor (Terminal) es virtualizado por lo que su gestión es más confiable. • Tener actualizados los contactos con los proveedores de servicios y partes. • Backup periódico de configuraciones, aplicaciones y datos. • Establecer puntos de restauración antes de realizar cambios. • Mantener actualizada la documentación de configuraciones, claves y funciones para cada servidor. • Solicitar al proveedor de hosting el servicio de monitoreo, que permita detectar fallas potenciales y atenderlas oportunamente. • Realizar copias espejo de los servidores. 	<ul style="list-style-type: none"> • Contactar al proveedor de hosting para que proporcione apoyo en la restauración del servidor. • Devolver la configuración del Sistema Operativo hasta el último punto de restauración funcional. • Si se tiene un servidor espejo, resolver el problema en el servidor caído, y volver a la operación normal. • En caso de tenerlo, habilitar el servidor de respaldo con el último backup de datos y configurar el acceso a este en los equipos clientes. Esto para el caso en que se estime que la puesta en marcha del servidor caído, sea superior a 1 día. • En caso de falla en componente de hardware, ordenar la compra y mientras su llegada se debe solicitar al proveedor la renta de un equipo o virtualización temporal. 	<ul style="list-style-type: none"> • Ingeniero de Desarrollo

- **Riesgo de falla en el fluido de energía eléctrica**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> • Picos de voltaje. • Altas o bajas de voltaje. • Interrupción del servicio eléctrico. 	<p>Grado de Impacto: Muy Alto</p> <p>Probabilidad de ocurrencia: Media</p>	<ul style="list-style-type: none"> • Los equipos de suministro eléctrico, deben estar conectados a la energía de emergencia del edificio. • Contar con UPS's que permitan regular el voltaje y proteger los equipos ante los sobre picos. • UPS's independientes en lo posible de larga duración para los servidores y los equipos de red. De lo contrario, que permita una autonomía suficiente para apagar los servidores en caso de cortes de energía prolongados. • Una vez se restablece el suministro eléctrico, esperar alrededor de 5 minutos antes de encender los equipos, para que se establezca la corriente eléctrica. 	<ul style="list-style-type: none"> • Acceder de inmediato al Data Center de la empresa para apagar los servidores adecuadamente. • Contactar al personal de mantenimiento del edificio, para que ponga en funcionamiento la planta de energía de emergencia. 	<ul style="list-style-type: none"> • Ingeniero de Soporte

- **Riesgo de fallas en los equipos eléctricos**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> • Falta de mantenimiento preventivo. • Desgaste de las baterías. • Mala calidad de la energía de entrada. • Mal uso de las salidas por conexión de equipos no soportados. 	<p>Grado de Impacto: Muy Alto</p> <p>Probabilidad de ocurrencia: Baja</p>	<ul style="list-style-type: none"> • Mantener vigentes las garantías y pólizas de mantenimiento. • Revisar la calidad de la energía en la acometida de entrada. • Monitorear y probar periódicamente los equipos de suministro eléctrico. • Programar mantenimiento preventivo anual. • Señalar las tomas de energía especificando el uso en cada caso. 	<ul style="list-style-type: none"> • Desviar el circuito eléctrico del equipo que salió de servicio, a una fuente de energía que cumpla los requisitos de calidad establecidos. • Contactar al proveedor correspondiente, para que reemplace o de mantenimiento al equipo dañado. 	<ul style="list-style-type: none"> • Ingeniero de Soporte

- **Riesgo de Incendio en la Oficina Principal**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> • Falta de mantenimiento preventivo de los equipos electrónicos • Sobrecargas eléctricas • Cortos Circuito 	<p>Grado de Impacto: Muy Alto</p> <p>Probabilidad de ocurrencia: Baja</p>	<ul style="list-style-type: none"> • Sistema detector de humo • Instalación de un número apropiado de extintores • Revisión periódica de la carga de extintores y su vencimiento • Programación de capacitaciones en el uso de elementos de seguridad y extintores • Eliminar del Data 	<ul style="list-style-type: none"> • Los brigadistas encargados deberán emplear los extintores buscando mitigar el fuego. • Los puntos remotos deberán operar • Permitir en el firewall el acceso del tráfico proveniente de cada una de las direcciones IP de los canales ADSL de los puntos remotos, generando una alternativa de conectividad. 	<ul style="list-style-type: none"> • Equipo de Sistemas

		Center cualquier material peligroso y promotor de incendio como papel, cartón, etc.		
--	--	---	--	--

• **Riesgo de Robo de Equipos**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> Fallas en el esquema de seguridad 	<p>Grado de Impacto: Muy Alto</p> <p>Probabilidad de ocurrencia: Muy Baja</p>	<ul style="list-style-type: none"> En Portería del Edificio de la Oficina Central se cuenta con vigilancia y cámaras de seguridad. En el piso de las Oficinas se cuenta con cámaras de seguridad, control de acceso mediante tarjeta de proximidad En el Data Center se maneja acceso con clave 	<ul style="list-style-type: none"> Si es robo de computadores se deberá proceder a rentar equipos Si es robo de servidores, se deberá rentar, realizar la instalación y restauración de los backups. 	<ul style="list-style-type: none"> Coordinador de Sistemas

• **Riesgo de Acceso no Autorizado de usuario Administrador**

CAUSA	VALORACIÓN DE SEVERIDAD	ACCIÓN DE MITIGACIÓN DE RIESGO	ACCION DE CONTINGENCIA	RESPONSABLE
<ul style="list-style-type: none"> Robo de la clave Falta de medidas de seguridad para el manejo de la clave 	<p>Grado de Impacto: Alto</p> <p>Probabilidad de ocurrencia:</p>	<ul style="list-style-type: none"> Solo el personal autorizado debe conocer la clave de Administrador La clave debe ser cambiada periódicamente Nunca se debe digitar la clave en presencia de otros. 	<ul style="list-style-type: none"> Realizar de inmediato el cambio de la clave del usuario Analizar el visor de eventos para determinar qué acciones no autorizadas o peligrosas realizó el usuario durante el acceso no autorizado. 	<ul style="list-style-type: none"> Coordinador de Sistemas Ingeniero de Desarrollo

	Baja	<ul style="list-style-type: none">• En caso de retiro de la compañía de un funcionario Administrador, se deben retirar los accesos y cambiar las claves.		
--	------	--	--	--

En todos los casos para activar el plan de contingencia es indispensable informar con prontitud a los usuarios y a las directivas de la compañía, la gravedad del daño presentado y el tiempo estimado para restaurar el servicio. Se debe hacer público un tiempo superior al que realmente se calcula, con el fin de dar una holgura para realizar los trabajos pertinentes de recuperación. Este aviso a las demás partes de la compañía, permite que cada área o departamento tome las medidas necesarias para la continuidad del negocio, que deben estar contempladas en el Plan de Contingencia Integral de la organización.

CAPITULO 4

4. PROPUESTA DE MEJORAMIENTO

Como resultado del proceso de consultoría se puede realizar una propuesta de mejoramiento soportada en los siguientes aspectos:

4.1. Servicio de mesa de ayuda

La función de la Mesa de Ayuda es proveer a los usuarios un punto único de contacto mediante el cual se resuelvan y/o canalicen sus necesidades relativas al uso de recursos y servicios TI, acuerdo al estándar definido por la empresa.

4.1.1. Objetivos de la mesa de ayuda

- Atender todas las llamadas recibidas.
- Resolver un alto porcentaje en línea.
- Seguimiento en línea de los casos derivados.
- Reducir llamados recurrentes en el tiempo.

4.1.2. Componentes del servicio

- Soporte al Sistema de Información: en este componente se reciben y canalizan todas las solicitudes que hacen referencia al sistema de información de la compañía (JD Edwards). Desde solicitudes de mantenimiento, requerimientos de desarrollo, verificación de errores, validaciones, etc.

- Soporte a la configuración: encargado de la gestión de la configuración de los componentes de TIC, tales como mantenimiento de usuarios, roles y permisos, actualizaciones, etc.
- Soporte de hardware: atención de solicitudes y programación de actividades que van desde mantenimientos preventivos, correctivos, requerimientos de equipos, capacitación básica a usuarios finales.
- Soporte de aplicaciones: enmarca los requerimientos sobre el software genérico con que cuenta la organización, como aplicaciones de ofimática, herramientas gráficas y de diseño, antivirus, etc.
- Soporte red de datos: recibe y canaliza todos los requerimientos de la red, adecuaciones, traslados, mantenimientos, instalaciones, configuraciones y gestión con los proveedores correspondientes.
- Soporte red de voz: atención a los requerimientos de la planta telefónica y demás servicios de mantenimiento, configuración y soporte de esta. Se encarga también de gestionar con el proveedor de comunicaciones, todos los servicios de voz contratados por la compañía.
- Monitoreo. Este componente tiene como responsabilidad el seguimiento mediante herramientas como consolas, toma de métricas y análisis de logs, para emitir alertas a las áreas correspondientes, de situaciones o comportamientos que puedan interferir en el normal desempeño de todos los elementos del engranaje de las tecnologías de información y telecomunicaciones de la empresa.

4.1.3. Estructura básica de la mesa de ayuda

En el Help Desk tradicional se diferencian los siguientes roles o cargos.

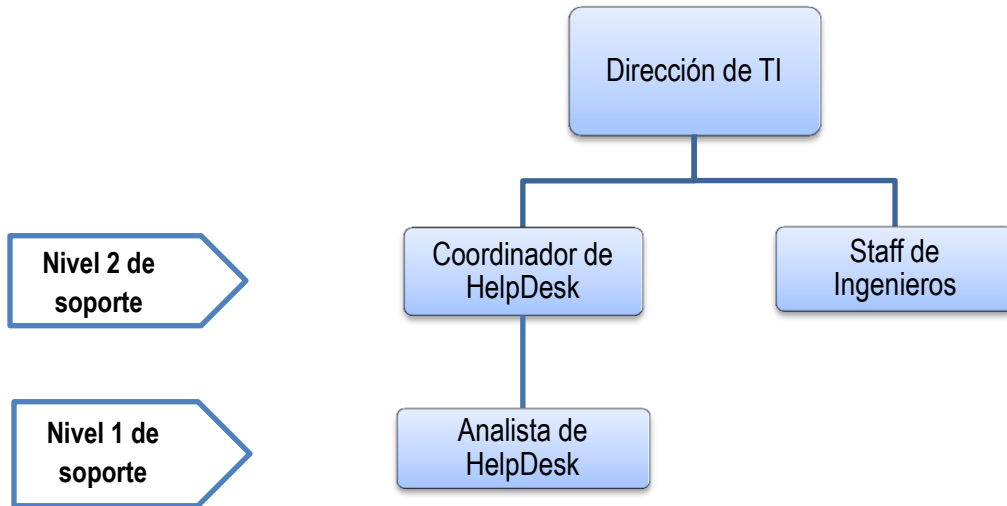


Figura 4.1. Estructura mesa de ayuda. **Fuente:** Los autores.

4.1.4. Responsables del servicio

Según las necesidades y la estructura orgánica de la empresa “T”, los roles sugeridos para la puesta en marcha de la mesa de ayuda son los siguientes:

Rol	Descripción
Analista de Help Desk.	Es el primer contacto de los usuarios con TI. Se encarga de dar solución de primer nivel a los requerimientos y de escalar a las áreas encargadas los incidentes de severidad 1 y 2. Programa las actividades preventivas y responde por el monitoreo y las métricas del servicio.
Staff de TI	Reciben de la mesa de ayuda los requerimientos de niveles superiores que por su complejidad y nivel de severidad, requieren ser atendidos por el respectivo dueño de servicio o transferidos a un tercero.

Dirección de TI	Como responsable de TI, modifica y mejora constantemente los servicios del Help Desk. Toma decisiones basadas en las métricas e indicadores de servicio. Evalúa el desempeño de los encargados de la mesa de ayuda. Verifica el cumplimiento de los tiempos pactados en los OLA's. Decide los cambios de personal.
-----------------	--

4.1.5. Matriz RACI

La matriz de asignación de responsabilidades (siglas de Responsable, Accountable, Consulted, Informed) muestra el rol que cada área debe desempeñar en las actividades planeadas. Con esta se pretende que cada uno de los actores involucrados, le de el alcance correspondiente a las tareas bajo su responsabilidad.

Actividad/Actor	Mesa de ayuda	Administrador del SI	Administrador Infraestructura	Dirección Mesa de Ayuda	Dirección TI
Soporte básico	R	A		I	
Soporte avanzado de hardware	R	A		I	
Soporte avanzado software	R	A		I	
Soporte avanzado sistema de información		R		A	I
Soporte básico hardware de servidores			R	A	I
Caída del sistema de información		C	C	R	A

R – Responsable: responsable de la ejecución del trabajo o de la tarea.

A - Accountable (Aprobador): asume la responsabilidad final por la correcta y completa ejecución de un proceso, recibiendo la información de los responsables de la ejecución del mismo.

C - Consulted (consultado): no está implicado directamente en la ejecución de un proceso pero da su opinión para la terminación de este.

I - Informed (informado): recibe la información de los avances y los resultados del trabajo.

4.1.6. Definición de los incidentes

Severidad	Descripción
1	Caída mayor de un sistema crítico que afecta a un gran número de usuarios o a una unidad de negocio. Impide el cumplimiento de los compromisos de la organización. Implicaciones financieras o legales.
2	Afectación a un sistema o aplicación, se puede usar pero con restricciones.
3	Incidentes que afectan a un número pequeño de usuarios. No impacta los niveles de servicio. Reportes que afectan la productividad de un solo usuario requiriendo instalaciones o reinstalaciones.
4	Incidentes que no afectan directamente la productividad de los usuarios. Existe una solución temporal disponible. Cambios de partes. Requerimientos de servicio.

4.1.7. Acuerdos de nivel de operación (OLA's)

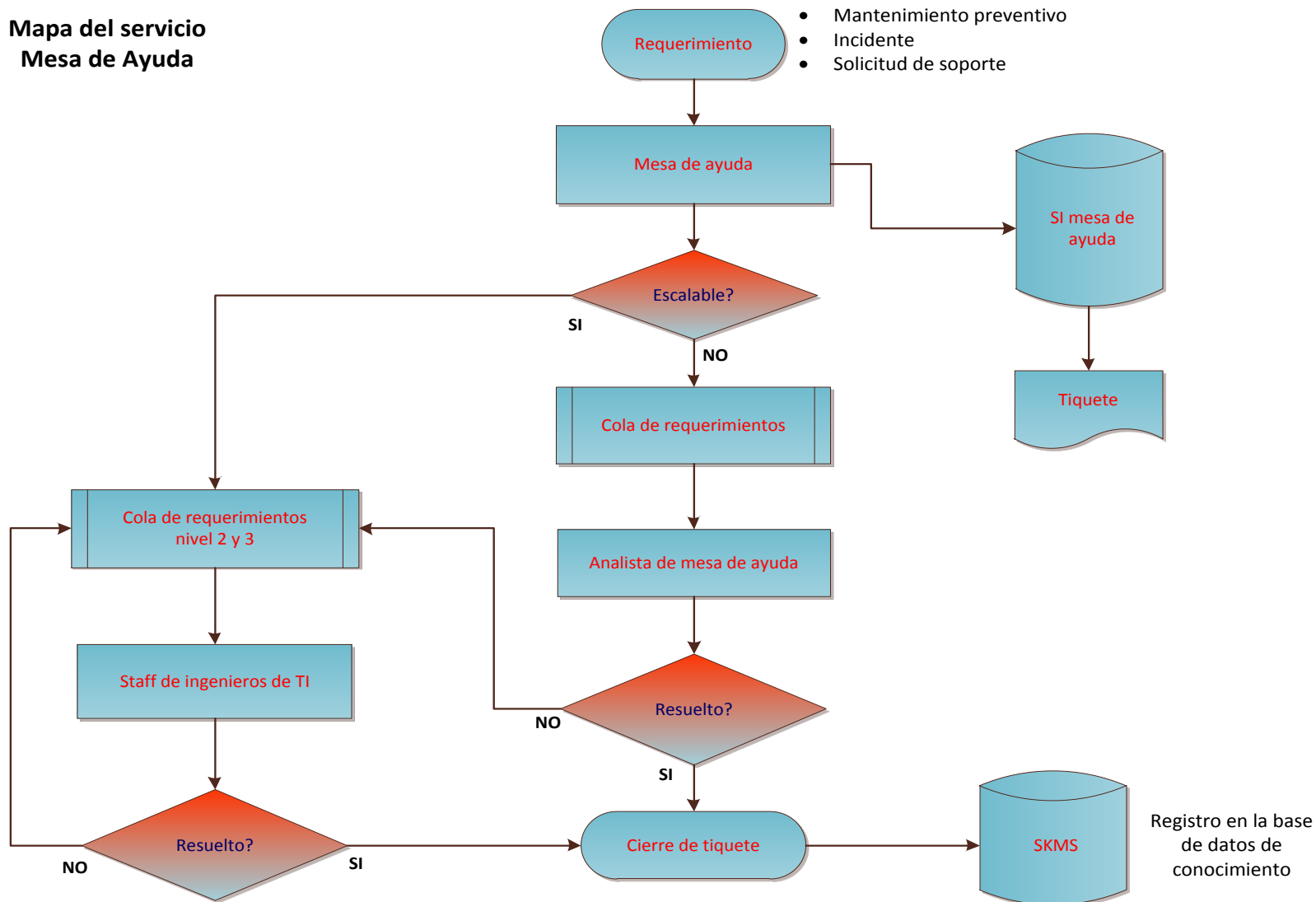
Ítem	Servicio	Descripción	Severidad	Nivel mínimo esperado	Responsables
1	Soporte básico	Tiempo de solución a una solicitud de soporte básica (no requiere cambios en el SW, BD o hardware).	4	Menor a 1 hora.	Mesa de ayuda

2	Soporte avanzado de hardware	Tiempo de solución a una solicitud de hardware. Requiere reinstalación de equipo de cómputo o cambio de componentes.	4	Menor a 8 horas.	Mesa de ayuda
3	Soporte avanzado software	Tiempo de solución a una solicitud de soportes avanzada (requiere cambios en el SW o en BD).	3	Menor a 1 día, después de la adquisición de repuestos.	Mesa de ayuda
4	Soporte avanzado sistema de información	Tiempo de solución a eventos en sistemas de información. Requiere apertura y cierre de bases de datos, o mantenimiento al software.	2	Menor a 2 horas.	Administrador del SI.
5	Soporte básico hardware de servidores	Tiempo de solución a un incidente menor de servidores.	2	Menor a 2 horas.	Administrador de infraestructura
6	Caída del sistema de información	Fallas eléctricas, de hardware o de la infraestructura que impiden la operación de los componentes del SI.	1	Menor a 1 hora.	

4.1.8. Mapa del servicio mesa de ayuda

Figura 4.2. Mapa del proceso mesa de ayuda. **Fuente:** los autores.

Mapa del servicio Mesa de Ayuda



4.2. Implementación de herramientas para gestión de TI

Como parte del proceso de desarrollo de la propuesta de mejoramiento, se establece realizar un estudio de la mejor opción para implementar en la compañía tres sistemas que permitan:

- Establecer mecanismos para un buen funcionamiento de la mesa de ayuda mediante una herramienta de Helpdesk con licencia gratuita.
- Realizar el monitoreo e inventario de Hardware y Software de la compañía, con el fin de determinar su uso real, bajo una herramienta con licencia gratuita.
- Dar soporte remoto a los equipos que se encuentran fuera de las instalaciones de la oficina principal, mediante un software de control remoto seguro y con la mejor relación costo/beneficio posible.

4.2.1. Sistema Help Desk

La compañía actualmente cuenta con sistema de generación de incidentes, problemas y demás, pero este se encuentra ligado directamente con el ERP, lo que impide el tratamiento de incidentes externos al ERP, por lo tanto se realizará la implementación de una herramienta que nos permita manejar de manera efectiva los requerimientos asociados al área de tecnología.

A continuación se describen las principales características, de los más importantes sistemas Help desk que se encuentran con licenciamiento gratuito.

ESPECIFICACIONES		Request Tracker	Spiceworks	Free Help Desk Software
Compañía		Best Practical Solutions, LLC	Spiceworks IT Software	iKode
Versión		v 4.0.1	v 5.0	v 3.1
Año Lanzamiento		1999	2006	
Modelo de despliegue	On Premise / Client Server	SI	SI	NO
	SaaS (Software as a Service)	NO	NO	SI
Licencia	Commercial	NO	NO	SI
	Open Source / Free	SI	SI	NO
	Proprietary	NO	SI	NO
Código Fuente Disponible		SI	NO	SI

REQUERIMIENTOS DE SISTEMA		Request Tracker	Spiceworks	Free Help Desk Software	
Plataformas para el cliente	Linux	SI	NO	SI	
	Mac	SI	SI	SI	
	Other	NO	NO	NO	
	Unix	SI	NO	NO	
	Windows	NO	SI	SI	
Plataformas para el Servidor	BSD	SI	NO	SI	
	Linux	NO	NO	SI	
	Mac OS X	SI	NO	NO	
	Solaris	SI	NO	NO	
	Unix	SI	NO	NO	
	Windows Home Server	NO	SI	NO	
	Windows Server 2003	NO	SI	NO	
	Windows Server 2008	NO	SI	NO	
	Lenguajes del lado del servidor	MS SQL	NO	NO	SI
		Microsoft SQL	NO	NO	NO

	Server			
	MySQL	SI	NO	NO
	Oracle	SI	NO	NO
	PostgreSQL	SI	NO	NO
	SMTP	NO	NO	SI
	SQL Server	NO	NO	SI
	sqlite	NO	SI	NO
Lenguaje de Implementación		Perl	Ruby on Rails	PHP

CARACTERISTICAS		Request Tracker	Spiceworks	Free Help Desk Software
Generales	Gestión de Activos	NO	SI	SI
	Reinicio de Contraseña automática	NO	SI	SI
	Facturación y Cartera	NO	SI	NO
	Control de Cambios	NO	SI	NO
	Administración de Contratos	NO	NO	SI
	Encuestas al cliente	NO	SI	NO
	Integración de Email	SI	SI	SI
	Administración de Incidentes, Problemas o solicitudes	SI	SI	NO
	Base de conocimientos y FAQ	NO	SI	SI
	Sincronización con directorio Activo	SI	SI	NO
	Integración móvil	SI	NO	NO
	Soporte Multi-sitio	NO	NO	NO
	Acceso a control remoto	NO	NO	NO
	Reporting	SI	SI	NO
	Reglas y Flujos	NO	SI	NO
	Calendarios y Programación	NO	NO	SI
	Personalización Disponible	Fondos	SI	NO
Imágenes de Botones		SI	NO	SI
Campos		SI	SI	NO
Fuentes		SI	NO	SI
Tablas		NO	SI	SI
Plantillas de diseño		NO	SI	SI
Maneras de realizar una solicitud	Email	SI	SI	SI
	Self-Service Portal	SI	SI	SI
Idioma	Español	SI	SI	NO
	Ingles	SI	SI	SI

		Request Tracker	Spiceworks	Free Help Desk Software
INFORMACIÓN ADICIONAL				
Tipo de Encriptación	AES	SI	NO	SI
	SSL	NO	SI	SI
Protocolo	Citrix ICA	NO	NO	SI
	Propietario	SI	SI	NO
Máximo número de computadores en el plan		3		
Mínimo número de computadores en el plan		1	1	

	Request Tracker	Spiceworks	Free Help Desk Software
PRECIOS			
Costo Inicial	US\$0	US\$0	US\$0
Costo Anual	US\$0	US\$0	US\$0
Costo Mensual	US\$0	US\$0	US\$0
Costo Host Anual	US\$0	US\$0	US\$39

Luego de verificar el comparativo, cuenta con grandes ventajas como la múltiple integración, sobre todo en cuanto al ingreso al sistema mediante el uso del directorio activo y el manejo de Tiquetes remotamente mediante el correo electrónico, se puede determinar que la mejor alternativa de software para implementar la solución de software es SPICEWORKS HELP DESK.

4.2.2. Inventarios de Hardware y Software

Actualmente la compañía lleva un control físico y manual acerca de los activos informáticos con los que cuenta, y el estado de los mismos se lleva en una hoja de Excel diligenciada manualmente. Por lo tanto es importante realizar el seguimiento de los activos y el monitoreo del software y archivos que contienen los equipos. Adicionalmente esto permite controlar el gasto por concepto de licenciamiento.

Para este proceso se han buscado herramientas con licencia gratuita que podamos implantar; sin embargo, se encuentran muchas herramientas pagas pero muy pocas bajo licenciamiento gratuito. La mejor opción que se ha detectado es SPICEWORKS INVENTORY, que permite realizar las funciones anteriormente descritas y además permite gran integración con el sistema de HelpDesk por ser del mismo fabricante.

4.2.3. Control remoto y soporte

Actualmente la compañía realiza los procesos de soporte informático con el uso de una herramienta que permite obtener el control de un computador remotamente, pero no se cuenta con el licenciamiento requerido, por lo que se trabaja con la versión de prueba. Buscando mejorar tal situación, se evaluarán a continuación algunas herramientas del mercado que nos permiten realizar este proceso, con los mejores servicios y la mejor relación costo/ beneficio.

Luego de buscar diferentes opciones en el mercado, se comparan las siguientes que podrían llegar a implementarse en la compañía.

ESPECIFICACIONES		TeamViewer	LogMeIn Pro	GoToMyPC Pro
Compañía		TeamViewer	LogMeIn	Citrix Online
Versión		v7	v2	v7
Año Lanzamiento		2005	2003	2002
SO Soportados	Linux	SI	SI	SI
	Mac	SI	SI	SI
	Other	SI	NO	NO
	Windows	SI	NO	NO
Plataforma Móvil	Android	SI	SI	NO
	iOS	SI	SI	NO
	Windows Mobile	NO	SI	NO

CARACTERÍSTICAS		TeamViewer	LogMeIn Pro	GoToMyPC Pro
------------------------	--	-------------------	--------------------	---------------------

Características de uso para usuario final	Soporte de Audio	SI	SI	NO
	Cortar, Copiar y Pegar	SI	SI	SI
	Encriptación	SI	SI	SI
	Transferencia de Archivos	SI	SI	SI
	Bloqueo de Teclado	SI	SI	SI
	Acceso Móvil	SI	SI	NO
	Impresión Remota	SI	SI	SI
	Blanqueamiento de Pantalla	SI	SI	SI
Características para Soporte	Solicitud de permiso de Acceso	SI	SI	NO
	Chat	SI	NO	NO
	Múltiples Monitores	SI	SI	SI
	NAT Passthrough	SI	SI	NO
	Asistencia Remota	SI	SI	NO
	Reporting	NO	SI	SI
	Ventana Transparente	SI	NO	SI
	Conexiones simultáneas ilimitadas	SI	NO	NO
Características soportadas	Brochures	SI	NO	NO
	Email	NO	NO	SI
	FAQ	NO	SI	SI
	Foros	NO	NO	SI
	Help Desk	NO	SI	SI
	Bases de Conocimiento	SI	SI	SI
	Chat	NO	NO	SI
	Manuales de usuario/propietario	SI	NO	NO
	Teléfono	SI	SI	SI
	Actualización del sistema	SI	NO	NO
	Guía de problemas	SI	NO	NO

INFORMACIÓN ADICIONAL		TeamViewer	LogMeIn Pro	GoToMyPC Pro
------------------------------	--	-------------------	--------------------	---------------------

Tipo de Encriptación	AES	SI	NO	SI
	SSL	NO	SI	SI
Protocolo	Citrix ICA	NO	NO	SI
	Propietario	SI	SI	NO
Máximo número de computadores en el plan		3		
Mínimo número de computadores en el plan		1	1	

	TeamViewer	LogMeIn Pro	GoToMyPC Pro
PRECIOS			
Costo Inicial	US\$2690		
Costo Anual		US\$3996	US\$9900
Costo Mensual		US\$676	US\$995

Luego de realizar la comparación tal y como se observa en la tabla anterior, se establece que la mejor alternativa para dar soporte es TeamViewer, principalmente basados en el hecho que soporta más sistemas operativos, cuenta con herramientas para informe mediante mail, transferencia de datos y chat, permite el acceso desde múltiples plataformas móviles como Android e iOS (Apple) y cuenta con un licenciamiento de por vida para el uso corporativo del software, de tal manera que únicamente se paga una cuota inicial.

4.3. Gestión administrativa

La consultoría realizada sobre el proceso de TI en la compañía "T" permitió identificar falencias en las áreas de organización y planeación de TICs. Teniendo en cuenta lo anterior, se sugiere adoptar algunas buenas prácticas de una guía o metodología que permita al Departamento de Sistemas operar eficazmente y realizar gestión sobre el trabajo realizado, de manera que se pueda promover la mejora continua y alinear la estrategia del área para apoyar el logro de los objetivos estratégicos de la organización.

Las buenas prácticas sugeridas como propuesta de mejoramiento para la empresa son:

- **Estructurar y organizar el área:** Es necesario definir la estructura interna del área, establecer la misión, las metas y los planes para alcanzarlas, los roles y asignación de responsabilidades.

- **Aseguramiento de la Calidad:** Se debe velar por implementar mecanismos o controles que permitan garantizar que las soluciones de software producto de desarrollo in house, cumplen satisfactoriamente los requerimientos previamente documentados y entregados por el cliente interno de la compañía, de manera que se logren reducir los reprocesos generados por modificaciones, ajustes y nuevas especificaciones efectuadas por el cliente cuando el software entra en producción, haciendo evidente una mala o incompleta definición del requerimiento.

- **Elaborar y realizar seguimiento a un Plan estratégico de TIC:** Se considera conveniente definir y compartir entre los miembros del Departamento de Sistemas, el plan estratégico de TIC, de manera que el equipo sume esfuerzos y trabaje conjuntamente para alcanzar una meta específica. Se debe hacer seguimiento periódico del alcance de las metas y de la alineación del trabajo realizado con las metas corporativas.

La definición del plan debe contemplar el estudio y monitoreo periódico de nuevas tendencias tecnológicas y regulaciones o aspectos legales que el área de TI deba tener en cuenta para fortalecer su operación y optimizar los resultados de la infraestructura de TI de la empresa.

- **Control de Ejecución de Presupuesto:** No es suficiente establecer un presupuesto anual de operación del área de TI; es necesario controlar periódicamente la ejecución del presupuesto, logrando identificar el estado de inversión, y detectar la causa de desfases presupuestales, si es que se presentan, de manera que se puedan analizar y generar experiencia a partir de estos, mejorando los presupuestos siguientes.

El análisis de la ejecución real permitirá encontrar oportunidades de mejora en la gestión de TI.

➤ **Evaluar madurez y estado informático de la empresa:** Es conveniente realizar evaluaciones en:

- control en la plataforma tecnológica y las aplicaciones
- Servicios tercerizados: hosting, colocation, canales de comunicaciones.
- Nivel de conocimiento y concientización de los usuarios.
- Controles físicos en las instalaciones
- Seguridad lógica en la plataforma de TI
- Nivel de documentación existente definido por políticas y procedimientos.

➤ **Definir políticas y procedimientos de TI:** Teniendo en cuenta que el nivel de políticas y procedimientos es mínimo y que desarrollar y divulgar estos puede permitir mejorar la visión de los clientes internos hacia el área y fortalecer la gestión se sugiere:

- Definir procedimientos a seguir en caso de contingencias
- Definir un plan de continuidad

- Definir procedimientos para gestión de usuarios.
 - Definir política de respaldo del personal de TI
 - Definir políticas de manejo y confidencialidad de la información de la compañía
 - Establecer un estándar o formato para definición de requerimientos de desarrollo
 - Establecer un estándar de documentación de desarrollo de software.
 - Definir niveles de servicio del área.
- **Planeación de capacitación del Recurso Humano de TI:** Se observa capacitación de los miembros del área. Sin embargo, no existe un plan o programa de capacitación que denote que estas son definidas estratégicamente o elegidas para fortalecer aspectos o minimizar carencias de conocimiento necesario para conseguir las metas del área.

Se deben establecer el alcance, los objetivos y participantes de la capacitación, elegir si se desea realizar capacitación interna o externa, presupuestar el costo, y planear oportunamente para evitar conflictos con períodos de alta carga laboral.

- **Establecer indicadores de gestión y evaluar desempeño:** El área no cuenta con indicadores de gestión o métodos de evaluación del desempeño, por lo que no hay manera de medir cuantitativa y

objetivamente el resultado de los miembros del equipo y del área. Se sugiere definir y establecer indicadores y mecanismos de evaluación.

Desarrollar y controlar un plan de contingencia: El área de TI debe definir, documentar y divulgar un plan de contingencia que permita retomar la operación en el menor tiempo posible, al presentarse algún incidente o situación que afecte la plataforma tecnológica de la compañía. Este plan deberá ser revisado periódicamente para analizar si se ajusta a las necesidades actuales de la organización y, si se requiere, actualizarse y divulgar dichas actualizaciones.

CONCLUSIONES

El desarrollo del proceso de consultoría de la infraestructura de TI y administración y mantenimiento del ERP en la compañía “T” resultó productivo del trabajo realizado por el equipo consultor en conjunto con los miembros del Departamento de Sistemas, lo que facilitó la labor y permitió transferir conocimiento a la organización, el cual se ve reflejado ahora en la habilidad adquirida por la empresa para analizar de manera autónoma el estado de su plataforma tecnológica y del servicio de TI percibido por los clientes, y la capacidad para generar las estrategias que buscan la mejora continua del servicio de TI.

En nuestro caso particular, la opinión más valiosa a la hora de evaluar el estado de madurez informática de la organización fue la del cliente del servicio de TI, recolectada a través de una encuesta que se analizó usando el modelo de madurez de Nolan adaptado por Fredy Reyes, con lo cual se identificó el estado real basado en argumentos y no en percepciones o ideas sesgadas del Departamento de Sistemas.

El estudio de metodologías para la administración, gestión y gobernabilidad de TI, permitió identificar deficiencias generadas por la falta de procedimientos, políticas y estándares, por lo que concluimos que se puede lograr una mejora sustancial adoptando recomendaciones de una guía de buenas prácticas ajustada a las necesidades particulares de la organización.

Cuando en una organización se decide establecer un plan de contingencia es necesario cumplir todas las etapas para ponerlo en marcha. No es suficiente definir una serie de acciones que quedan en la cabeza de los empleados y que en realidad nadie tiene claras. Es indispensable formular, documentar, divulgar y probar el plan e incluso actualizarlo cuando así se requiera. Solo de esta manera

el plan de contingencia podrá tener éxito cuando se presente un incidente, y tendrá vida propia sin depender de la memoria del recurso humano que puede además tener una alta rotación o cambio en las organizaciones actuales.

Adicionalmente, como parte del desarrollo de la consultoría, se establecieron algunas sugerencias para sistematizar sistemas de requerimientos, soporte remoto y monitoreo e inventario de hardware y software de la compañía, basados en las necesidades específicas de la compañía. Teniendo en cuenta las mismas, se buscaron alternativas open source con el fin de que la empresa no incurra en gastos innecesarios para help desk, y monitoreo e inventario de hardware y software. Para el caso de soporte remoto se sugirió una herramienta paga pero con grandes prestaciones que se ve representado en la relación costo - beneficio.

BIBLIOGRAFÍA

Meza, Francisco, Obregón Miguel (1997). Manual de Formación de Consultoría. IBM Educación.

Reyes, Fredy (2011). Indicadores para el Diagnostico de Madurez Informática. Guías de Clase del módulo de Gerencia de Sistemas Informáticos. Especialización de Gerencia Informática. Universidad EAN.

Tieneke Verheijen, Annelies Van Der Veen, Ruby Tjassing, Mike Pieper, Axel Kolthof, Arjen de Jong, & Jan Van Bon. (2010). Fundamentos de ITIL V3. Van Haren publishing.

FICHA BIBLIOGRÁFICA DEL TRABAJO

Tipo	Trabajo dirigido
Título	Propuesta de mejoramiento y contingencia de sistemas informáticos
Modalidad programa	Postgrado, Gerencia Informática
Edición	Bogotá, D.C., Universidad EAN, 2012
Autores	Yohana Ramírez; Andrés Gómez; Edwin Londoño.
Palabras clave	Consultoría informática. Plan de contingencia. Metodologías de gestión informática. Evaluación de madurez informática.
Descripción	Este trabajo analiza la situación actual de TIC de la empresa constructora "T", con el propósito de mejorar los procesos existentes y aprovechar las herramientas tecnológicas, para generar valor a la organización.
Fuentes	<p>Textos de Consulta:</p> <ul style="list-style-type: none"> • Meza, Francisco; Obregón Miguel (1997). Manual de Formación de Consultoría. IBM Educación. • Reyes, Fredy (2011). Indicadores para el Diagnostico de Madurez Informática. Guías de Clase del módulo de Gerencia de Sistemas Informáticos. Especialización de Gerencia Informática. Universidad EAN. • Tieneke Verheijen, Annelies Van Der Veen, Ruby Tjassing, Mike Pieper, Axel Kolthof, Arjen de Jong, & Jan Van Bon. (2010). Fundamentos de ITIL V3. Van Haren publishing. <p>Sitios Web:</p> <ul style="list-style-type: none"> • Universidad de Medellín, Centro Integral de Asesoría y Consultoría. http://www.udem.edu.co/UDEM/Extension/CentroAsesoriasCo

	<p>nsultorias/infoInteres.htm</p> <ul style="list-style-type: none"> • Álvarez, Luis F; Zayas Enrique; Pérez Marisol. Consultoría Organizacional. http://www.monografias.com/trabajos15/consultoria-organizacional/consultoria-organizacional.shtml • Álvarez, Luis F (2005). Proceso de Consultoría Organizacional. http://www.gestiopolis.com/recursos4/docs/ger/econsultoria.htm • Codina, Alexis (2006). La consultoría: difusión de tecnología y formación gerencial. http://www.degerencia.com/articulo/la_consultoria_difusion_de_tecnologia_y_formacion_gerencial • Álvarez, Luis F (2005). Proceso de consultoría organizacional. http://www.gestiopolis.com/recursos4/docs/ger/econsultoria.htm • Francavilla, Carlos (2009). Problemas de TI. http://cafrancavilla.wordpress.com/tag/problemas-it • Fundación Iberoamericana del Conocimiento. Modelo Nonaka. http://www.gestiondelconocimiento.com/modelo_nonaka.htm • Canales, Roberto (2005). Calidad en el desarrollo de Software. CMMI. http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=cmmi • Tamayo, Alonso; Tamayo Johnny (2006). Guía para la formulación de un Plan de Contingencias. http://www.cibersociedad.net/congres2006/gts/comunicacion.php?id=309 • Secure and IT Proyectos (2012). ITIL / ISO 20000. http://www.secureit.es/index.php?page=seguridad&subpage=iso20k • Osiatis S.A. ITIL – Gestión de Servicios de TI.
--	--

	<p>http://itil.osiatis.es/Curso_ITIL</p> <ul style="list-style-type: none"> • Find the best (2012). Compare Help Desk Software http://help-desk-software.findthebest.com/compare/15-17-59/Request-Tracker-vs-Spiceworks-vs-Free-Help-Desk-Software • Spiceworks (2012). Free PC & Network Inventory Software. http://www.spiceworks.com/free-pc-network-inventory-software/ • Find the best (2012). Compare Remote Desktop Software. http://remote-desktop.findthebest.com/compare/1-3-23/TeamViewer-vs-LogMeIn-Pro-vs-GoToMyPC-Pro
Contenido	El trabajo se encuentra dividido en cuatro capítulos así: Capítulo1: Análisis y diagnóstico de la situación actual del Departamento de sistemas y su rol en la organización. Capítulo 2: Identificación de procesos y metodologías de TIC's necesarios para la mejora. Capítulo 3: Generación de Propuesta de plan de contingencia. Capítulo 4: Generación de Propuesta de mejoramiento.
Metodología	Consultoría informática.
Conclusiones	Ver capítulo: Conclusiones.
Periodo académico	2012-2

ANEXO 1

Resultados de la encuesta a usuarios y lideres de área

La encuesta realizada durante los primeros quince días el mes de mayo de 2012, a los empleados de la empresa constructora, tenía como fin medir la percepción de los usuarios de los sistemas de información y las tecnologías de comunicaciones, hacia los servicios, el uso y el enfoque de estos al interior de la compañía. Para esto se clasificaron las preguntas en 4 categorías que evalúan igual número de aspectos tendientes a encontrar el nivel de madurez a partir del punto de vista de los clientes del departamento de sistemas.

Los usuarios se dividieron en dos grupos: los empleados de oficina y salas de venta de rango medio que usan equipos de computo para sus labores, y los lideres de cada departamento. A ambos grupos se les realizaron las mismas preguntas. La clasificación en dos grupos se justifica en la óptica que tiene cada uno de estos sobre los aportes que la tecnología como herramienta y medio de trabajo aporta al desempeño de la compañía.

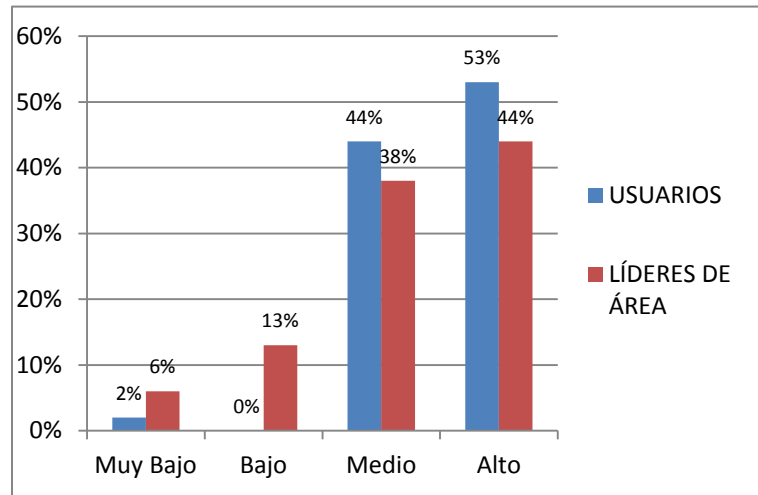
Relación de la encuesta con la calificación de Madurez Informática

Áreas de evaluación	Ítems de evaluación	Preguntas que apoyan la calificación
Tecnologías	Grado de cubrimiento en la organización	1-5-6
	Dominio de los usuarios	2-12
	Soporte del área informática	4
	Evaluación del soporte a la gestión de los sistemas de información.	3
Motivaciones.	Motivaciones de la Organización hacia la Informática	De la 7 a la 9.
Nivel de Participación y Asimilación de las TIC por los usuarios	Promotores del uso de TIC	10
	Integración de usuarios en los servicios de TIC	13
	Habilidad para la gestión de la información	12
	Nivel de resistencia al cambio	11
Carácter de la Gerencia Informática	Capacidad de alineación e interdependencia de la estrategia de TIC con la estrategia organizacional	15-14
	Capacidad del talento humano de GI en aspectos técnicos	16
	Capacidad del talento humano de GI en gestión de servicios (al cliente interno)	17-18

Desarrollo de la encuesta

Tecnologías:

1. Teniendo en cuenta los procesos realizados en la empresa, considera que el apoyo brindado por las tecnologías es:



2. Para cada una de las siguientes herramientas tecnológicas, evalúe el apoyo que le prestan para el desarrollo de su trabajo:

Equipos de informática y software básico		
	Usuarios	Lideres de área
Muy Baja	0%	0%
Baja	2%	6%
Media	31%	26%
Alta	63%	68%
(No aplica)	4%	0%

Comunicaciones y redes		
	Usuarios	Lideres de área
Baja	2%	18%
Media	21%	25%
Alta	73%	57%
(No aplica)	4%	0%

Sistemas de información (JDE, Zue, CIO)		
	Usuarios	Lideres de área
Muy Baja	0%	0%
Baja	2%	0%
Media	8%	32%
Alta	67%	37%
(No aplica)	23%	31%

3. La frecuencia con la que los problemas que se presentan en su trabajo están ligados a fallas en cada una de las siguientes tecnologías de informática y comunicaciones es:

Equipos de informática y software básico		
	Usuarios	Lideres de área
Muy Baja	13%	31%
Baja	40%	39%
Media	22%	18%

Alta	17%	12%
(No aplica)	8%	0%

Comunicaciones y redes		
	Usuarios	Lideres de área
Muy Baja	22%	19%
Baja	41%	51%
Media	20%	18%
Alta	11%	12%
(No aplica)	6%	0%

Sistemas de información (JDE, Zue, CIO)		
	Usuarios	Lideres de área
Muy Baja	6%	0%
Baja	29%	37%
Media	25%	32%
Alta	16%	6%
(No aplica)	24%	25%

4. La efectividad que recibe del soporte del área de Sistemas para el manejo de cada una de las siguientes tecnologías es:

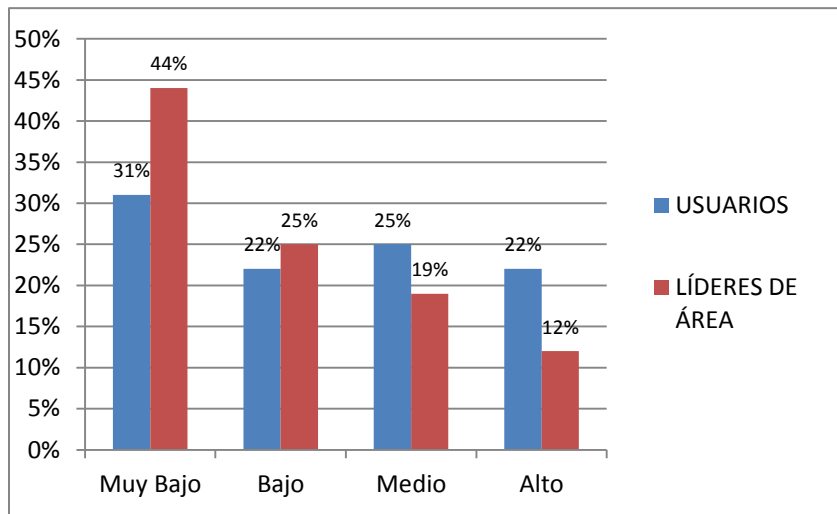
Equipos de informática y software básico		
	Usuarios	Lideres de área
Muy Baja	0%	6
Baja	2%	6
Media	33%	18
Alta	61%	68
(No aplica)	4%	0%

Comunicaciones y redes		
	Usuarios	Lideres de área
Muy Baja	0%	0%
Baja	2%	6%
Media	20%	25%
Alta	74%	69%
(No aplica)	4%	0%

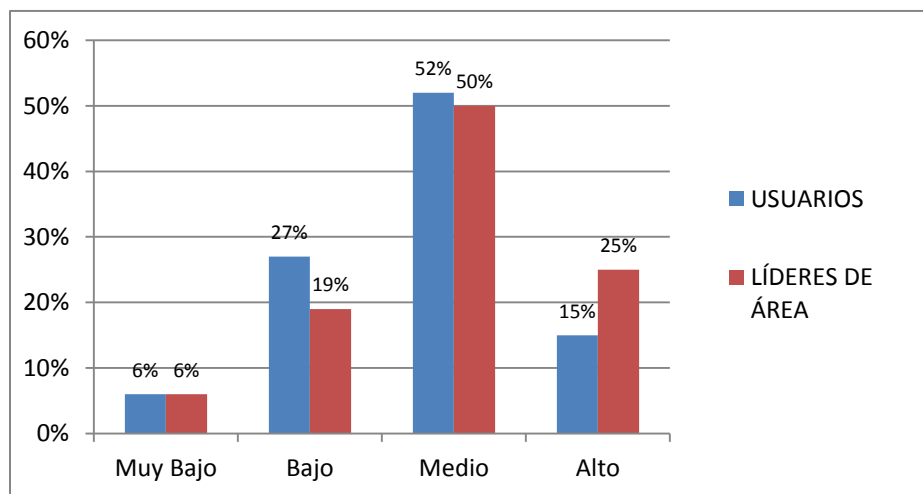
Sistemas de información (JDE, Zue, CIO)		
	Usuarios	Lideres de área
Muy Baja	0%	0%
Baja	0%	0%
Media	4%	25%

Alta	74%	50%
(No aplica)	22%	25%

5. Con qué frecuencia la información contenida en un sistema, tiene que ser transferida a otro:

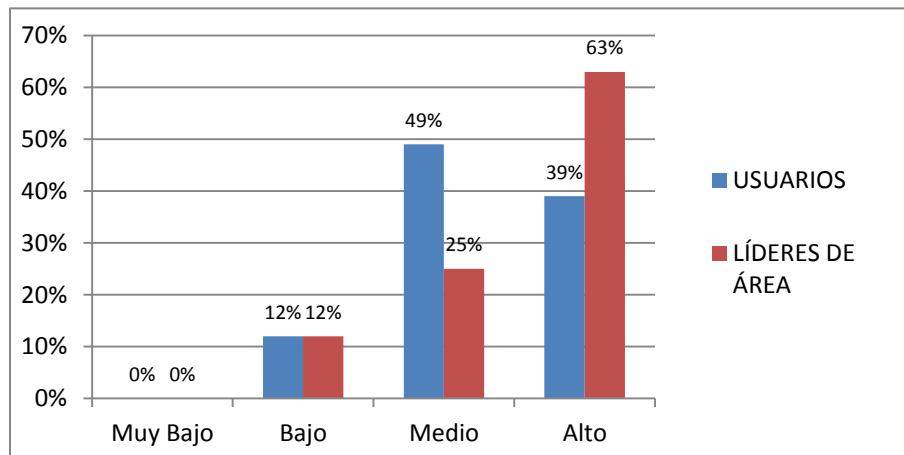


6. Con qué facilidad puede consultar información de su interés que ha sido ingresada por otros usuarios u otras áreas:

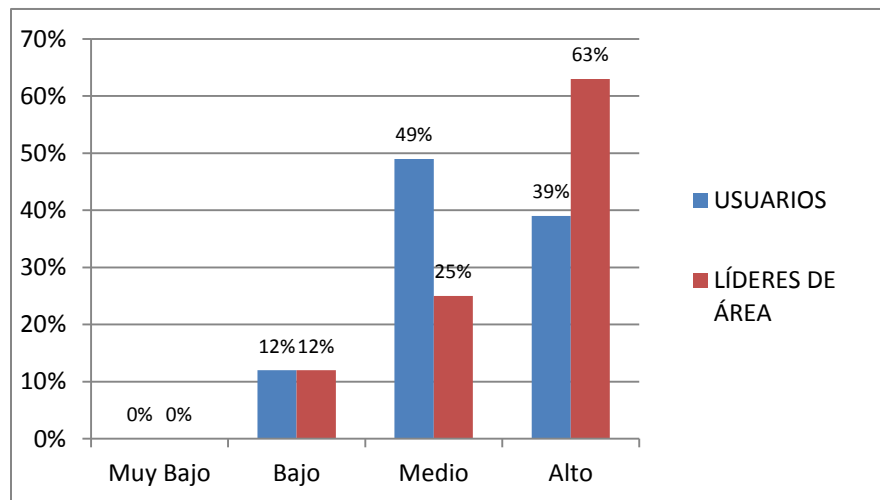


Motivaciones:

7. El interés de la organización por motivar el uso de las tecnologías de información y comunicación para facilitar las actividades laborales es:



8. En su opinión, el nivel de inversión que la empresa realiza en tecnología es:



9. Considera que la decisión de la empresa de invertir en herramientas tecnológicas y de comunicaciones se debe principalmente a:

	Usuarios	Lideres de área
Reducir costos y optimizar la operación empresarial.	6%	6%
Minimizar riesgos de operación de la empresa y no quedarse atrás con respecto a la competencia.	14%	6%
Proporcionar herramientas para tomar decisiones y facilitar el desarrollo y crecimiento de la empresa.	70%	75%
Desarrollar estrategias innovadoras y marcar la diferencia con respecto a la competencia.	10%	13%

Nivel de Aceptación y Asimilación de las TIC por los usuarios:

10. En la empresa, quienes más promueven el uso de las Tecnologías de Información y Comunicación son:

	Usuarios	Lideres de área
Los funcionarios del área de Sistemas	9%	7%
Los usuarios	7%	7%
Entre ambos (funcionarios de Sistemas y usuarios) por necesidad.	48%	50%
Entre ambos (funcionarios de Sistemas y usuarios) en pro de mejorar.	36%	36%

11. Considera que su grado de aceptación frente a nuevas Tecnologías de Información y Comunicación para el desarrollo de su trabajo, en las siguientes categorías es:

Equipos de informática y software básico		
	Usuarios	Lideres de área
Muy Baja	0%	0%
Baja	2%	0%
Media	36%	15%
Alta	60%	85%
(No aplica)	2%	0%

Comunicaciones y redes		
	Usuarios	Lideres de área
Muy Baja	0%	0%
Baja	0%	15%
Media	29%	7%
Alta	67%	78%
(No aplica)	4%	0%

Sistemas de información (JDE, Zue, CIO)		
	Usuarios	Lideres de área
Muy Baja	2%	0%
Baja	0%	0%
Media	17%	28%

Alta	59%	43%
(No aplica)	22%	29%

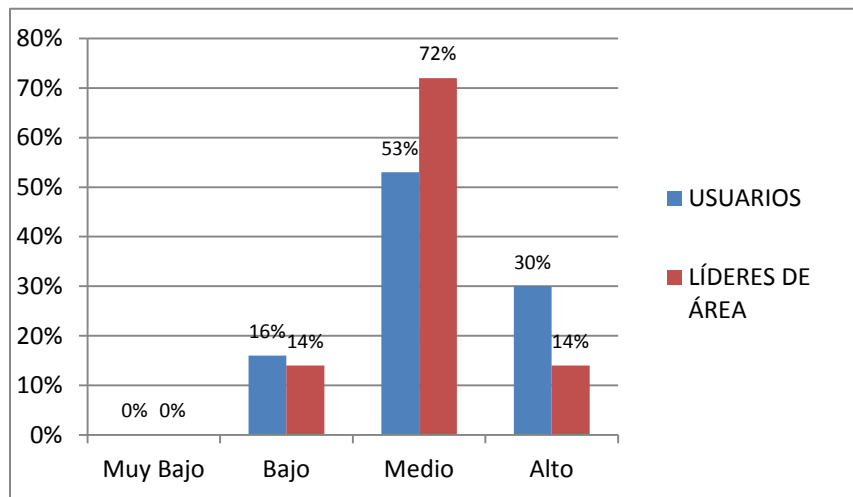
12. Considera que su dominio de cada una de las siguientes herramientas tecnológicas y de comunicaciones es:

Equipos de informática y software básico		
	Usuarios	Lideres de área
Muy Baja	0%	0%
Baja	4%	0%
Media	62%	72%
Alta	34%	28%
(No aplica)	0%	0%

Comunicaciones y redes		
	Usuarios	Lideres de área
Muy Baja	0%	0%
Baja	4%	7%
Media	60%	79%
Alta	32%	14%
(No aplica)	4%	0%

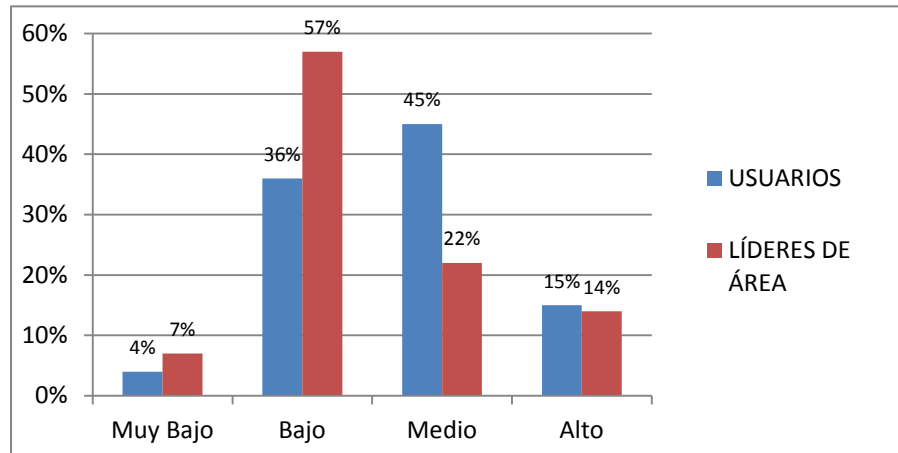
Sistemas de información (JDE, Zue, CIO)		
	Usuarios	Líderes de área
Muy Baja	0%	14%
Baja	2%	14%
Media	46%	51%
Alta	29%	7%
(No aplica)	23%	14%

13. Su capacidad de generar soluciones a problemas cotidianos apoyado en los servicios de Informática y comunicaciones ha sido:

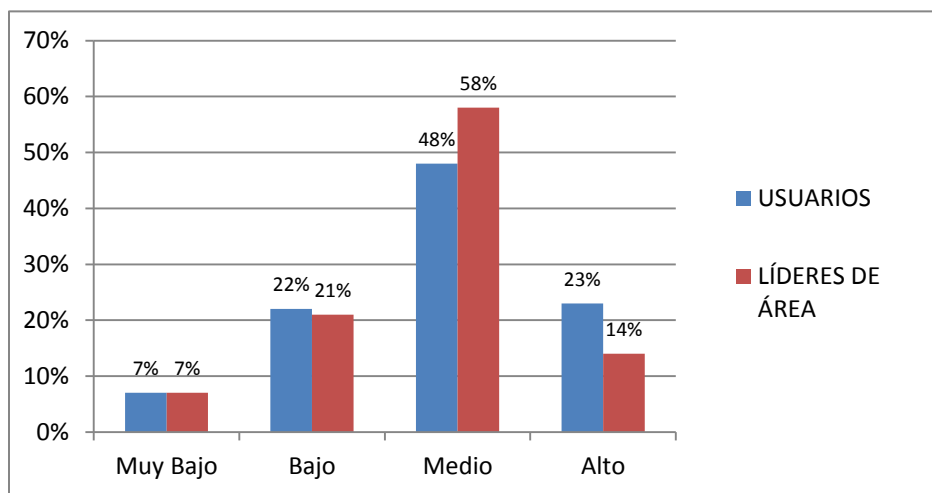


Carácter del área de sistemas:

14. La frecuencia con la que el desarrollo de tareas propias de su área requiere la intervención del personal de Sistemas es:



15. En qué nivel considera que los programas de capacitación realizados por la empresa buscan que los empleados aprovechen al máximo las herramientas tecnológicas en sus actividades laborales:



16. La frecuencia con la que el personal de Sistemas resuelve de manera oportuna los incidentes, en cada una de las siguientes herramientas tecnológicas es:

Equipos de informática y software básico		
	Usuarios	Lideres de área
Muy Baja	0%	7%
Baja	4%	7%
Media	40%	29%
Alta	54%	57%
(No aplica)	2%	0%

Comunicaciones y redes		
	Usuarios	Lideres de área
Muy Baja	0%	7%
Baja	4%	7%
Media	30%	36%
Alta	61%	50%
(No aplica)	5%	0%

Sistemas de información (JDE, Zue, CIO)		
	Usuarios	Lideres de área
Muy Baja	0%	7%
Baja	2%	0%

Media	4%	29%
Alta	69%	42%
(No aplica)	25%	22%

17. Al evaluar si el personal de Sistemas resuelve de manera oportuna los incidentes en cada una de las siguientes herramientas tecnológicas, qué calificación daría:

Equipos de informática y software básico		
	Usuarios	Lideres de área
Muy Baja	0%	7%
Baja	2%	7%
Media	37%	21%
Alta	57%	65%
(No aplica)	4%	0%

Comunicaciones y redes		
	Usuarios	Lideres de área
Muy Baja	0%	7%
Baja	2%	7%
Media	28%	36%
Alta	66%	50%
(No aplica)	4%	0%

Sistemas de información (JDE, Zue, CIO)		
	Usuarios	Lideres de área
Muy Baja	0%	7%
Baja	1%	0%
Media	7%	22%
Alta	70%	50%
(No aplica)	22%	21%

18. La calidad en el servicio al cliente que usted percibe por parte del área de Sistemas en cada una de las siguientes tecnologías es:

Equipos de informática y software básico		
	Usuarios	Lideres de área
Muy Baja	0%	7%
Baja	0%	7%
Media	27%	15%
Alta	71%	71%
(No aplica)	2%	0%

Comunicaciones y redes		
	Usuarios	Lideres de área
Muy Baja	0%	7%
Baja	2%	7%
Media	18%	21%
Alta	76%	65%

(No aplica)	4%	0%
-------------	----	----

Sistemas de información (JDE, Zue, CIO)		
	Usuarios	Lideres de área
Muy Baja	0%	7%
Baja	0%	0%
Media	2%	21%
Alta	74%	51%
(No aplica)	24%	21%

ANEXO 2

Documento de requerimientos

1. DATOS GENERALES				
Versión:	[x.x]	Solicitante:	[nombre]	
Identificador del requerimiento:	[REQ-xxx]	Nombre del requerimiento:	[nombre]	
Tipo de requerimiento:	Especificación/Diseño/ Desarrollo/ Ajustes	Estado:	Estado	Fecha
			Recibido	
			Detallado	
			Aprobado	
			Rechazado	
			En ejecución	
			Entregado	
Responsable:				
Área responsable:				

2. HISTORIAL DE REVISIONES			
Fecha	Versión	Cambios en la versión	Autor
[dd/mm/aaaa]	[x.x]	[detalles]	[nombre]

3. DESCRIPCIÓN DEL PROBLEMA	
Aplicación:	
Modulo:	

Descripción del problema:	
Descripción de la solución:	
Sistemas de información relacionados:	
Alcance de la solución:	

4. FIRMA ACEPTACIÓN	
Área usuaria	Área informática

ANEXO 3

Documento de planeación

1. DATOS GENERALES				
Versión:	[x.x]	Solicitante:	[nombre]	
Identificador del documento:	[PLR-xxx]	Requerimiento asociado:	[REQ-xxx]	
Tipo de requerimiento:	Especificación/Diseño/ Desarrollo/ Ajustes	Estado:	Estado	Fecha
			Recibido	
			Detallado	
			Aprobado	
			Rechazado	
			En ejecución	
			Entregado	
Responsable:				

2. HISTORIAL DE REVISIONES			
Fecha	Versión	Cambios en la versión	Autor
[dd/mm/aaaa]	[x.x]	[detalles]	[nombre]

3. OBJETIVOS A PLANEAR	
Objetivo específico:	
Objetivos generales:	

4. DETALLE PLANEACIÓN						
Componente	Complejidad del cambio	Horas	Jornadas	Responsable	Rol	% ejecutado

5. FIRMA ACEPTACIÓN	
Responsable planeación	Responsable desarrollo

ANEXO 4

Formato gestión de cambios

1. DATOS GENERALES			
Versión:	[x.x]	Solicitante:	[nombre]
Identificador del requerimiento:	[GC-xxx]	Requerimiento asociado:	[REQ-xxx]
Responsable:			
Área responsable:			

2. HISTORIAL DE REVISIONES			
Fecha	Versión	Cambios en la versión	Autor
[dd/mm/aaaa]	[x.x]	[detalles]	[nombre]

3. DESCRIPCIÓN DEL PROBLEMA	
Aplicación:	
Módulo:	
Objetos y/o componentes sujetos a cambio(s):	
Descripción del cambio(s):	
Estado actual del cambio(s):	

4. FIRMA ACEPTACIÓN	
Revisor	Aceptación

ANEXO 5

Documento de pruebas

1. DATOS GENERALES			
Versión:	[x.x]	proyecto:	[nombre]
Identificador del documento:	[PRU-xxx]	Requerimiento asociado:	[REQ-xxx]
		Estado:	Estado
Responsable Diseño:			Recibido
			Diseñado
			Ejecutado
Responsable Ejecución:			Aprobado
			Rechazado
			En ejecución

2. HISTORIAL DE REVISIONES			
Fecha	Versión	Cambios en la versión	Autor
[dd/mm/aaaa]	[x.x]	[detalles]	[nombre]

3. VERIFICACIÓN DE PRUEBAS				
Casos de validación exitosos				
Descripción	Datos carga	Resultado esperado	Resultado obtenido	Observaciones

Casos de validación fallidos				
Descripción	Datos carga	Resultado esperado	Resultado obtenido	Observaciones

4. OBSERVACIONES GENERALES	
Observaciones favorables	Observaciones desfavorables
Conclusiones	

5. FIRMA ACEPTACIÓN	
Ejecutor de pruebas	Evaluador documento

ANEXO 6

Documento de capacitación.

1. DATOS GENERALES				
Versión:	[x.x]	Solicitante:	[nombre]	
Identificador del documento:	[OT-xxx]	Nombre del entrenamiento:	[nombre]	
Tipo de entrenamiento:	Presencial externo/ Presencial interno/ online / autodidacta/ semi-presencial	Estado:	Estado	Fecha
			Recibido	
			Aprobado	
			Realizado	
			En ejecución	
Rechazado				
Responsable:				
Área responsable:				
Entidad/Persona capacitadora:				

2. HISTORIAL DE REVISIONES			
Fecha	Versión	Cambios en la versión	Autor
[dd/mm/aaaa]	[x.x]	[detalles]	[nombre]

3. DETALLES DEL ENTRENAMIENTO	
Aplicaciones asociadas:	
Modulos asociados:	

Motivo entrenamiento:	
Fechas:	
Horarios:	
Costos:	
Tema general:	
Detalles temas a tratar:	
Asistentes:	

4. FIRMA ACEPTACIÓN
Área aprobadora

ANEXO 7

Acta de reunión

1. DATOS GENERALES			
Versión:	[x.x]	proyecto:	[nombre]
Identificador del documento:	[ACR -xxx]	Requerimiento asociado:	[REQ-xxx]
Elaborado por:			

2. DETALLES REUNIÓN			
Referencia:		Fecha:	
Empresas:			
Asistentes a la reunión:			
Próxima reunión:			

3. ORDEN DEL DÍA

4. RESULTADOS REUNIÓN	
Asuntos tratados y acuerdos	Responsables y fechas

5. FIRMA ACEPTACIÓN	
<i>[Parte 1]</i>	<i>[Parte 2]</i>
<i>[Parte 3]</i>	<i>[Parte 4]</i>

ANEXO 8

Adquisición de software

1. DATOS GENERALES			
Versión:	[x.x]	proyecto:	[nombre]
Identificador del documento:	[AHS-xxx]	Requerimiento asociado:	[REQ-xxx]
Descripción del uso del software o hardware:			
Recursos con los que se adquiere el software o hardware:			

2. HISTORIAL DE REVISIONES			
Fecha	Versión	Cambios en la versión	Autor
[dd/mm/aaaa]	[x.x]	[detalles]	[nombre]

3. INFORMACIÓN TÉCNICA HARDWARE			
No. Equipos:		Equipo:	
Modelo:			
Características técnicas:			
Garantía:		Software a utilizar en el equipo:	

4. INFORMACIÓN TÉCNICA SOFTWARE			
Software:		Versión:	
Página Web:		No. Licencias:	
Tipo de licencia:	Perpetua / Anual / Actualización / otra		

5. JUSTIFICACIÓN (Características relevantes que necesita y no son cumplidas por el software libre):

6. FIRMA ACEPTACIÓN	
Solicitante	Aprobador

LICENCIA DE USO – AUTORIZACIÓN DE LOS AUTORES

Actuando en nombre propio identificado (s) de la siguiente forma:

Nombre Completo EDWIN ALBERTO LONDOÑO RUA

Tipo de documento de identidad: C.C. T.I. C.E. Número: 71.760.634

Nombre Completo JAIRO ANDRES GÓMEZ GÓMEZ

Tipo de documento de identidad: C.C. T.I. C.E. Número: 1.010.168.168

Nombre Completo MARITZA YOHANA RAMÍREZ ROBAYO

Tipo de documento de identidad: C.C. T.I. C.E. Número: 52.717.302

Nombre Completo _____

Tipo de documento de identidad: C.C. T.I. C.E. Número: _____

El (Los) suscrito(s) en calidad de autor (es) del trabajo de tesis, monografía o trabajo de grado, documento de investigación, denominado:

PROPUESTA DE MEJORAMIENTO Y CONTINGENCIA DE SISTEMAS
INFORMÁTICOS EN LA EMPRESA "T"

Dejo (dejamos) constancia que la obra contiene información confidencial, secreta o similar: SI NO
(Si marqué (marcamos) SI, en un documento adjunto explicaremos tal condición, para que la Universidad EAN mantenga restricción de acceso sobre la obra).


Por medio del presente escrito autorizo (autorizamos) a la Universidad EAN, a los usuarios de la Biblioteca de la Universidad EAN y a los usuarios de bases de datos y sitios webs con los cuales la Institución tenga convenio, a ejercer las siguientes atribuciones sobre la obra anteriormente mencionada:


- A. Conservación de los ejemplares en la Biblioteca de la Universidad EAN.
- B. Comunicación pública de la obra por cualquier medio, incluyendo Internet
- C. Reproducción bajo cualquier formato que se conozca actualmente o que se conozca en el futuro
- D. Que los ejemplares sean consultados en medio electrónico
- E. Inclusión en bases de datos o redes o sitios web con los cuales la Universidad EAN tenga convenio con las mismas facultades y limitaciones que se expresan en este documento
- F. Distribución y consulta de la obra a las entidades con las cuales la Universidad EAN tenga convenio


Con el debido respeto de los derechos patrimoniales y morales de la obra, la presente licencia se otorga a título gratuito, de conformidad con la normatividad vigente en la materia y teniendo en cuenta que la Universidad EAN busca difundir y promover la formación académica, la enseñanza y el espíritu investigativo y emprendedor.

Manifiesto (manifestamos) que la obra objeto de la presente autorización es original, el (los) suscritos es (son) el (los) autor (es) exclusivo (s), fue producto de mi (nuestro) ingenio y esfuerzo personal y la realizó (zamos) sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de exclusiva autoría y tengo (tenemos) la titularidad sobre la misma. En vista de lo expuesto, asumo (asumimos) la total responsabilidad sobre la elaboración, presentación y contenidos de la obra, eximiendo de cualquier responsabilidad a la Universidad EAN por estos aspectos.

En constancia suscribimos el presente documento en la ciudad de Bogotá D.C.,

NOMBRE COMPLETO: EDWIN ALBERTO LONDOÑO
FIRMA: 
DOCUMENTO DE IDENTIDAD: 71.760.634
FACULTAD: POSTGRADOS
PROGRAMA ACADÉMICO: GERENCIA INFORMATICA

NOMBRE COMPLETO: Jairo Andrés Gómez
FIRMA: 
DOCUMENTO DE IDENTIDAD: 1.010.168.168
FACULTAD: POSTGRADOS
PROGRAMA ACADÉMICO: GERENCIA INFORMATICA

NOMBRE COMPLETO: MARITZA JOHANA RUIZ
FIRMA: 
DOCUMENTO DE IDENTIDAD: 52.717.302
FACULTAD: POSTGRADOS
PROGRAMA ACADÉMICO: GERENCIA INFORMATICA

NOMBRE COMPLETO: _____
FIRMA: _____
DOCUMENTO DE IDENTIDAD: _____
FACULTAD: _____
PROGRAMA ACADÉMICO: _____

Fecha de firma: 14 SEPTIEMBRE 2012