ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

ELABORACIÓN DE UN PROCESO PARA EVALUAR EL DESEMPEÑO DE LAS EMPRESAS DESARROLLADORAS DE SOFTWARE, EN CUANTO A LAS OPERACIONES DE TI UTILIZANDO COBIT 4.0

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

CARRANZA MORALES MERY GUADALUPE

m.sheins@gmail.com

SAQUINGA SANGUCHO MARITZA XIMENA

ximemaritza@gmail.com

DIRECTOR: MSc. ING. JAIME NARANJO

jfna@epn.edu.ec

QUITO, DICIEMBRE 2008

DECLARACIÓN

Nosotros, Mery Guadalupe Carranza Morales y Maritza Ximena Saquinga Sangucho, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Mery Guadalupe Carranza Morales

Maritza Ximena Saquinga Sangucho

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Mery Guadalupe Carranza Morales y Maritza Ximena Saquinga Sangucho,, bajo mi supervisión.

MSc. Inng. Jaime Naranjo

DIRECTOR DE PROYECTO

CONTENIDO

INDICE TABLAS

INDICE DE FIGURAS

RESUMEN

En la presente tesis se elabora un proceso para evaluar el desempeño de las empresas desarrolladoras de software, en cuanto a las operaciones de TI utilizando COBIT 4.0

Comenzamos con el capítulo 1, planteando que al presente en muchas de las empresas sus mas grandes activos son la información y la tecnología con la que cuentan, además de justificar el uso de COBIT 4.0 con una revisión de los conceptos del estándar propuesto para este proyecto, con el fin de entender los diferentes procesos que involucra el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que éstas implican.

En el capítulo 2, se realiza el análisis del medio para lo cual se determina el universo de empresas desarrolladoras de software existentes en la cuidad de Quito, consecutivamente como el universo de empresas desarrolladoras es muy amplio, se selecciona una muestra representativa de la misma utilizando métodos estadísticos.
Se plantea la ejecución del estudio de la muestra seleccionada para lo cual se escoge como instrumento la encuesta, la misma que se aplica en la muestra seleccionada.
Luego de tabular los datos de los resultados obtenidos de las encuestas realizadas, se procede a realizar el análisis de resultados para lo cual se tomara como referencia el cuadro de interpretación conforme lo sugiere COSO. Y en base a este análisis y al nivel de importancia de los procesos del COBIT 4.0, se considera la acción que se debe tomar según la interpretación (baja, media, alta).

En el capítulo 3, fundamentados en el trabajo realizado en el segundo capítulo se elabora el proceso, y se detalla los pasos a seguir para la ejecución del mismo.

En el capítulo 4, se escoge una empresa caso estudio y aplica el proceso en base al tercer capítulo.

Finalmente en el capítulo 5, se presentan las conclusiones y recomendaciones obtenidas como resultado de la realización de este trabajo

CAPÍTULO 1: PLANTEAMIENTO DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

En la actualidad, para muchas empresas, la información y la tecnología con la cuentan, representan sus más valiosos activos. Por lo tanto reconocen los beneficios de la tecnología de información y la utilizan para impulsar el desarrollo de las mismas.

El caso de estudio seleccionado para el desarrollo de nuestra investigación son las empresas desarrolladoras de software ubicadas en la cuidad de Quito. Con la finalidad de plantear la elaboración de un proceso para evaluar el desempeño de estas empresas, en cuanto a sus operaciones de TI, tomando como referencia la metodología COBIT 4.0

COBIT es una metodología aceptada mundialmente para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que éstas implican. La metodología COBIT se utiliza para planear, implementar, controlar y evaluar el gobierno de TI; incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.

COBIT ofrece un conjunto de mejores prácticas aceptadas internacionalmente de forma general que permiten a los directivos, ejecutivos y gerentes aumentar el valor de TI y reducir los riesgos relacionados. Puesto que el marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.
Las características principales del marco de trabajo COBIT son, de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

“La nueva edición de COBIT contiene prácticas y enlaces que dan soporte a los requisitos de gobierno de TI de ejecutivos y directivos, enlazando también con las bases para satisfacer los requisitos más detallados de los responsables de la instalación de la solución y el suministro del servicio. Así se consigue dar un mayor soporte a la optimización de las

inversiones TI, asegurar la consolidación de los valores y mitigar el riesgo de TI de forma transparente."[1]

La edición COBIT 4.0 se concentra más en las empresas y en las responsabilidades de directivos y empleados, siempre en evolución. COBIT 4.0 es la primera actualización importante del núcleo desde el lanzamiento de la tercera edición de COBIT en el año 2000. "COBIT 4.0 no se parece en nada a un tomo académico; hay material útil en todas las páginas". "Posee el potencial de ser un documento útil para cualquier situación."[2]

COBIT 4.0 incluye una guía para directivos y todos los niveles de gestión. Se compone de cuatro secciones:

- La visión general ejecutiva
- La estructura
- El núcleo (objetivos de control, directivas de gestión y modelos de madurez)
- Apéndices (mapas, referencias cruzadas y un glosario)

El núcleo se divide según los 34 procesos TI y contiene una definición completa del control, gestión y medida de cada proceso.
Además, COBIT 4.0:

- Analiza cómo pueden trazarse mapas de objetivos de control de los cinco dominios de gobierno TI para identificar vacíos potenciales
- Ajusta y traza mapas entre COBIT y otras normativas (ITIL, CMM, COSO, PMBOK, ISF e ISO 17799)
- Clarifica las relaciones entre el indicador de objetivo clave (key goal indicator, KGI) y el indicador de rendimiento clave (key performance indicator, KPI), identificando cómo los KPI permiten conseguir los KGI
- Enlaza los objetivos empresariales con los objetivos TI y los procesos TI (una investigación detallada en ocho sectores permite evaluar cómo los procesos COBIT facilitan el logro de objetivos TI específicos y, por extensión, de objetivos empresariales)

[1] Erik Guldentops, CISA, CISM, consultor de gestión en Bruselas, Bélgica, y miembro del equipo de desarrollo COBIT desde su creación.
[2] Christopher Fox, de ACA.

A partir de estos aspectos ya mencionados se señala entonces el objeto de estudio para esta investigación, que consiste en establecer una comparación de los procesos que se realizan en las empresas desarrolladoras de software con cada uno de los procesos y subprocesos planteados en COBIT 4.0

Con intención de direccionar metodológicamente la investigación, se formula la siguiente interrogante con sentido de apoyo y orientación al proceso investigativo, a fin de facilitar a las empresas desarrolladoras de software un proceso que les permita evaluar sus operaciones de TI.
¿Cual de los procesos y/o subprocesos citados en el COBIT 4.0 son aplicables a empresas desarrolladoras de software?

1.2 JUSTIFICACIÓN DEL USO DEL MODELO COBIT 4.0

Actualmente las organizaciones ya están interesadas en la aplicación del marco de trabajo o el gobierno de TI de COBIT 4.0. Por lo tanto, puede este proyecto convertirse en un marco de referencia, específicamente para empresas desarrolladoras de software, ya que se reducirá los procesos del COBIT 4.0 ajustándose solo a dichas empresas, y facilitando las tareas de los administradores de las operaciones de TI. Esta investigación servirá como base para el desarrollo de nuevas versiones debido a que la metodología COBIT se actualiza constantemente.

COBIT contribuye a reducir las brechas existentes entre los objetivos de negocio, y los beneficios, riesgos, necesidades de control y aspectos técnicos propios de un proyecto TI; proporcionando un Marco Referencial Lógico para su dirección efectiva.
La metodología COBIT

El marco referencial conceptual de la metodología COBIT proporciona una visión integral, capaz de responder a las necesidades de directivos, usuarios (de diverso nivel) y auditores (internos y externos).

Se busca enlazar los objetivos empresariales con los objetivos TI y los procesos TI. En la práctica esto se logra identificando los 1). Requerimientos del negocio para la información y los 2) recursos de TI que son impactados en forma primaria por cada objetivo de control, asociado a cada 3) proceso TI.

1. Requerimientos de negocio para la información:
    - Efectividad
    - Eficiencia
    - Confidencialidad
    - Integridad
    - Disponibilidad
    - Cumplimiento
    - Confiabilidad
2. Recursos TI:
    - Datos
    - Aplicaciones
    - Tecnología
    - Instalaciones
    - Personal
3. Procesos de TI: Son 4 dominios en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI:
    - Planear y Organizar
    - Adquirir e Implementar
    - Entregar y Dar Soporte
    - Monitorear y Evaluar

Asociados a los 4 dominios existen 34 procesos de alto nivel, desagregados en 302 procesos y/o actividades menor jerarquía.

Para cada proceso de alto nivel existen objetivos, medidas de control de diversa naturaleza, indicadores asociados (de objetivo clave -key goal indicator, KGI- y de rendimiento clave -key performance indicator, KPI-), además de modelos de madurez.

Para cada medida de control se lleva a cabo una clasificación dentro del marco referencial COBIT:

- Primario: es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.
- Secundario: es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.
- Blanco (vacío): podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

A su vez cada proceso y/o actividad de menor jerarquía involucra una sumatoria de buenas prácticas necesarias de considerar para el cumplimiento de los requisitos de control exigidos para cada caso, estableciendo los resultados deseados o propósitos a ser alcanzados mediante su implementación.

Adicional al Marco Referencial, COBIT dispone también de Guías de Auditoría, las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los 302 objetivos detallados de control recomendados para proporcionar a la gerencia certeza o una recomendaciones de mejoramiento.

Incorpora además de un Conjunto de Herramientas de Implementación, la cual proporciona:

- Una Síntesis Ejecutiva, que permite a la alta gerencia conciencia y entendimiento de COBIT.
- Casos de estudio y lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente.
- Diversas herramientas, tales como: Diagnóstico de la Conciencia de la Gerencia (Management Awareness Diagnostic) y el Diagnóstico de Control de TI (IT Control Diagnostic).
- Adicionalmente, se incorporan preguntas y respuestas más frecuentes acerca de COBIT y varias presentaciones para distintos niveles jerárquicos y audiencias dentro de las organizaciones.

CAPÍTULO 2: ANALISIS DEL MEDIO

Para realizar el análisis del medio en primera instancia se busco el universo de empresas desarrolladoras de software existentes en la cuidad de Quito, tomando como referencia los datos obtenidos en la Superintendencia de Compañías, siendo un total de 368 empresas.

Posteriormente como el universo de empresas desarrolladoras es muy amplio, seleccionamos una muestra representativa de la misma utilizando métodos estadísticos.

2.1 DETERMINACIÓN DEL TAMAÑO Y SELECCIÓN DE LA MUESTRA REPRESENTATIVA

2.1.1 DETERMINACIÓN DEL UNIVERSO

Para poder determinar el universo se han seguido los siguientes pasos:

a) En la presente investigación se ha identificado como nuestro punto de estudio a las empresas desarrolladoras de software de la cuidad de Quito; que ha sido determinado como el *universo*.
b) A continuación se redactó una carta dirigida a la SUPERINTENDENCIA DE COMPAÑIAS en la cual se solicitaba que se remita un listado de empresas desarrolladoras de software de la ciudad de Quito, al mismo tiempo que se ponía énfasis en que la información proporcionada sería exclusivamente para uso académico.
c) La SUPERINTENDENCIA DE COMPAÑIAS nos proporcionó un listado de todas las empresas que están relacionadas con la informática y computación, con información muy general la cual constaba de campos como: nombre de la compañía, provincia, cuidad, dirección, teléfono y actividad económica, este listado contenía 734 empresas.
d) Una vez que contamos con la lista de empresas que están relacionadas con la informática y computación, se clasifico a dichas empresas según la actividad económica que este acorde a las empresas desarrolladoras de software, entonces se

determino que el universo de empresas desarrolladoras de software es 368 (VER ANEXO 1).

2.1.2 DETERMINACIÓN DEL TAMAÑO DE LA MUESTRA

Para poder determinar el tamaño de la muestra se recurrió a la estadística, específicamente a la teoría de Muestreo Proporcional.

Se encontró la siguiente ecuación la misma que determinará el tamaño de la muestra asociada a la población antes encontrada.

$$n = \frac{N * Z^2_{\alpha/2} * P * (1-P)}{(N-1) * e^2 + Z^2_{\alpha/2} * P * (1-P)}$$ [1]

Donde:

N = Tamaño del universo,

$Z_{\alpha/2}$ = variable estandarizada de distribución normal,

P = Proporción de una categoría de la variable,

e = Error máximo,

n = tamaño de la muestra.

Para definir el tamaño de la muestra vamos a tomar en consideración una confiabilidad del 95% entonces con este dato, en conjunto con la tabla de probabilidad acumulada de la ley de distribución normal estándar[2], tenemos que el valor de la variable $Z_{\alpha/2} = 1.69$.

También tomaremos como dato que el 90% de las empresas contestan nuestras encuestas, lo que equivale a P = 0.90; nuestro margen de error propuesto será del 10%, el cual es recomendado para este tipo de investigación, esto nos da como dato e = 0.10.
Con nuestro tamaño de población N = 368, procedemos a calcular el tamaño de la muestra.

---

[1] Formula matemática del muestreo aleatorio; tomada del libro Estadística para la Administración y la Ingeniería, GALINDO D

[2] Probabilidad acumulativa de 00 a z para la distribución normal estándar; tomada del libro Estadística para la Administración y la Ingeniería, GALINDO D. Edwin; página 427.

$$n = \frac{368 * 1.69^2 * 0.9 * (1 - 0.9)}{(368 - 1) * 0.1^2 + 1.69^2 * 0.9 * (1 - 0.9)}$$

$$n = 24{,}087$$

El muestreo tiene por objeto examinar una parte representativa de la población, e inferir resultados para aplicarlos a la población completa.[1]

Por lo tanto el tamaño de la muestra resultante es de 24 empresas desarrolladoras de software que van a ser analizadas y estudiadas.

2.2 PLAN DE EJECUCIÓN DEL ESTUDIO DE LA MUESTRA SELECCIONADA

2.2.1 SELECCIÓN DE TÉCNICA E INSTRUMENTOS DE RECOLECCIÓN DE DATOS.

La técnica e instrumento escogido es la **encuesta**. Ya que con esta podemos obtener información precisa y tener mayor contacto con las empresas y el personal que las integran.

2.2.2 DESCRIPCIÓN DEL PROCEDIMIENTO.

El procedimiento que nosotros realizamos consta de los siguientes pasos y actividades:

2.2.2.1 Visita a las empresas seleccionadas

En cada una de las empresas objeto de investigación, se realizó una entrevista previa, a una persona considerada clave, gerentes generales, gerentes medios, dueños de la empresa en la

[1] Conceptos Básicos de los elementos de Muestreo, tomada del libro Estadística para la Administración y la Ingeniería, GALINDO D. Edwin; página 353.

cuál se realizará una exposición sobre los objetivos de nuestra investigación y los resultados que se obtendrá al fin de la misma.

2.2.2.2 Preparación de la encuesta

La encuesta está basada en encuestas presentadas en anteriores proyectos de titulación y en la información que queremos obtener sobre procesos que se realizan en el área de TI (VER ANEXO 2).

2.3 EJECUCIÓN DEL PLAN Y OBTENCIÓN DE RESULTADOS

2.3.1 EJECUCIÓN DEL PLAN

A continuación detallamos cual fue el procedimiento que se llevo a cabo para la ejecución del plan:

- En cada una de las empresas desarrolladoras de software escogidas para nuestro estudio realizamos llamadas telefónicas para confirmar la fecha y hora para realizar las visitas.
- En la visita se procedió a dar una breve introducción sobre el contenido de la encuesta y su objetivo. Previo a la realización de la misma se tomo muy en cuenta el cargo y perfil, ya que debíamos diferenciar el grado de conocimiento que tiene cada uno de los miembros de la empresa, y encaminar al más indicado para llenar las encuestas.

Cabe destacar que existieron varios obstáculos para cumplir con nuestro objetivo, puesto que en lo referente al manejo de la información las empresas, tienen desconfianza y no acceden fácilmente a proveer información y más cuando hablamos de auditoría.

2.3.2 OBTENCIÓN DE RESULTADOS

A continuación se detallan los resultados obtenidos y el análisis de los mismos de las encuestas realizadas a las 24 empresas desarrolladoras de software.

La información será clasificada, con la ayuda de gráficos que nos facilitará a posteriori el análisis.

Establecemos una clasificación por bloques de acuerdo a cada una de las preguntas planteadas en la encuesta.

2.3.2.1 Resultados obtenidos de la encuesta

- ***Resultados obtenidos para el proceso PO1: Definir un plan estratégico de TI***

TOTAL	SI	PARCIALMENTE	NO
24	14	9	1

Tabla 1: Resultado del análisis del proceso: Definir un plan estratégico de TI.

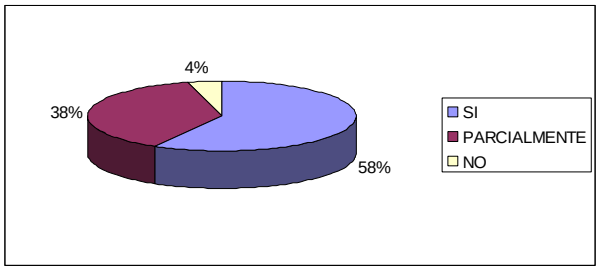


Figura 1: Definir un plan estratégico de TI.

- ***Resultados obtenidos por el proceso PO2: Definir la arquitectura de información***

Modelo de la arquitectura de información empresarial

TOTAL	SI	PARCIALMENTE	NO
24	19	5	0

Tabla 2: Resultado del análisis del proceso: Modelo de la arquitectura de información empresarial

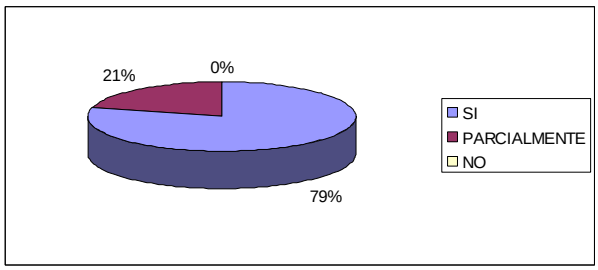


Figura 2: Modelo de la arquitectura de información empresarial

Diccionario de datos empresarial y reglas de sintaxis de datos

TOTAL	SI	PARCIALMENTE	NO
24	6	14	4

Tabla 3: Resultado del análisis del proceso: Diccionario de datos empresarial y reglas de sintaxis de datos

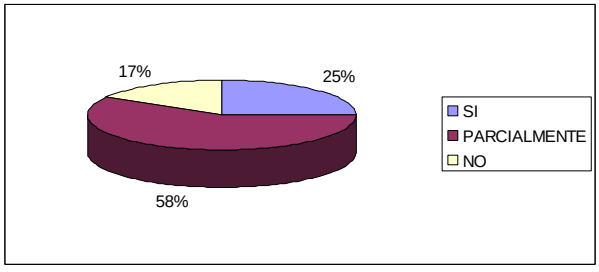


Figura 3: Diccionario de datos empresarial y reglas de sintaxis de datos

- ***Resultados obtenidos por el proceso PO3: Determinar la dirección tecnológica***

TOTAL	SI	PARCIALMENTE	NO
24	19	5	0

Tabla 4: Resultado del análisis del proceso: Determinar la dirección tecnológica

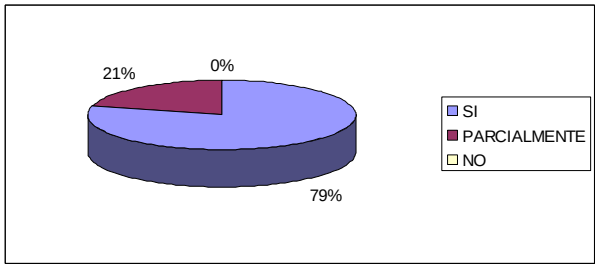


Figura 4: Determinar la dirección tecnológica

- ***Resultados obtenidos por el proceso PO4: Definir los procesos, organización y relaciones de TI***

TOTAL	SI	PARCIALMENTE	NO
24	18	4	2

Tabla 5: Resultado del análisis del proceso: Definir los procesos, organización y relaciones de TI.

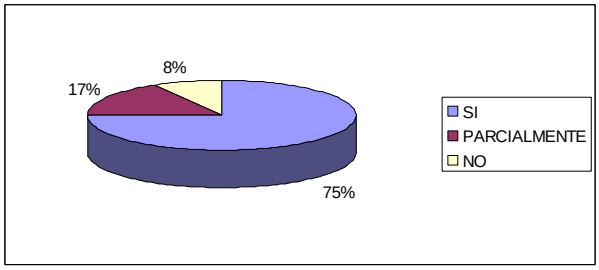


Figura 5: Definir los procesos, organización y relaciones de TI

- ***Resultados obtenidos por el proceso PO5: Administrar la inversión en TI.***

TOTAL	SI	PARCIALMENTE	NO
24	13	7	4

Tabla 6: Resultado del análisis del proceso: Administrar la inversión de TI.

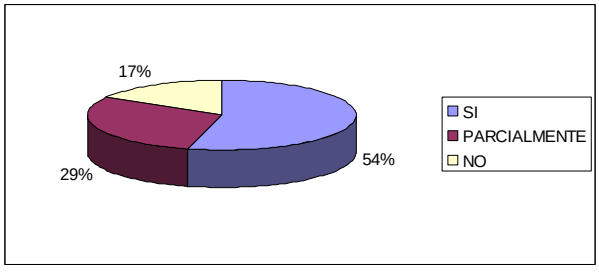


Figura 6: Administrar la inversión de TI.

- ***Resultados obtenidos por el proceso PO6: Comunicar las aspiraciones y la dirección de la gerencia.***

  Implantación de políticas de TI

TOTAL	SI	PARCIALMENTE	NO
24	13	7	4

Tabla 7: Resultado del análisis del proceso: Implantación de políticas de TI

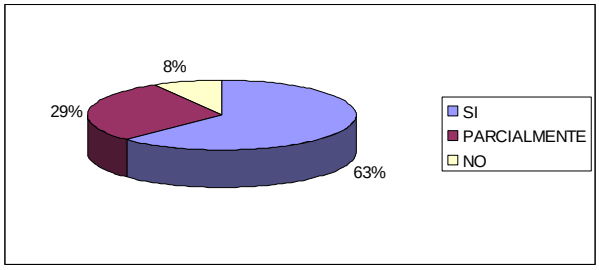


Figura 7: Implantación de políticas de TI.

Administración de políticas para TI

TOTAL	FRECUENTEMENTE	AVECES	CASI NUNCA
24	6	8	0

Tabla 8: Resultado del análisis del proceso: Administración de políticas para TI

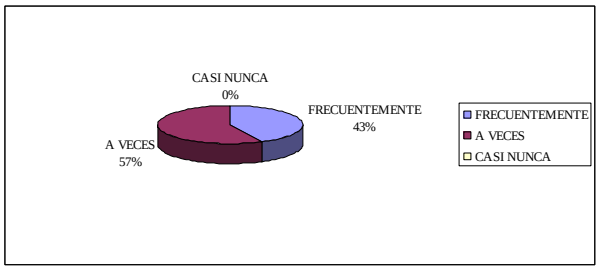


Figura 8: Administración de políticas para TI.

- ***Resultados obtenidos por el proceso PO7: Administrar recursos humanos de TI.***

  Entrenamiento del personal de TI

TOTAL	SI	PARCIALMENTE	NO
24	7	13	4

Tabla 9: Resultado del análisis del proceso: Administrar recursos humanos de TI.

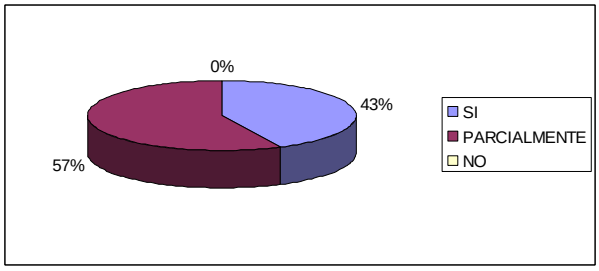


Figura 9: Entrenamiento del personal de TI.

- ***Resultados obtenidos por el proceso PO8: Administrar la calidad.***

TOTAL	SI	PARCIALMENTE	NO
24	16	5	3

Tabla 10: Resultado del análisis del proceso: Administrar la calidad.

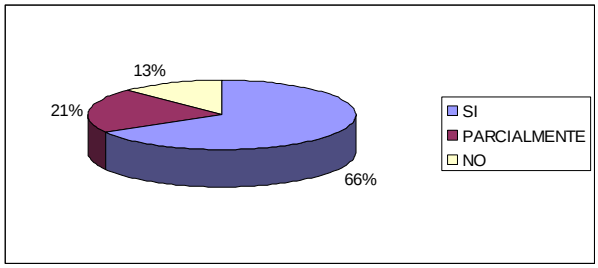


Figura 10: Administrar la calidad.

- ***Resultados obtenidos por el proceso PO9: Evaluar y administrar riesgos de TI.***

Identificación de eventos

TOTAL	SI	PARCIALMENTE	NO
24	10	13	1

Tabla 11: Resultado del análisis del proceso: Identificación de eventos.

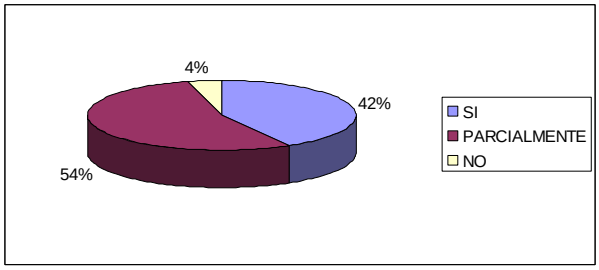


Figura 11: Iidentificación de eventos.

Respuesta a los riesgos

TOTAL	SI	PARCIALMENTE	NO
24	16	8	0

Tabla 12: Resultado del análisis del proceso: Respuesta a los riesgos

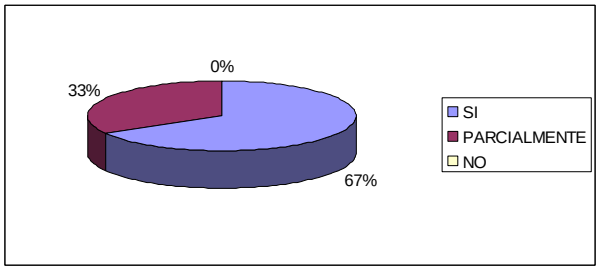


Figura 12: Respuesta a los riesgos.

- ***Resultados obtenidos por el proceso PO10: Administrar proyectos.***

TOTAL	SI	PARCIALMENTE	NO
24	9	13	2

Tabla 13: Resultado del análisis del proceso: Administrar proyectos.

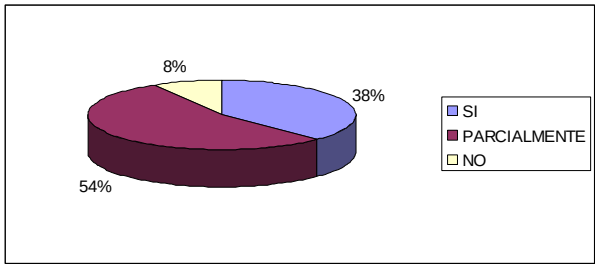


Figura 13: Administrar proyectos

- ***Resultados obtenidos por el proceso AI1: Identificar soluciones automatizadas.***

Estudio de factibilidad y formulación de cursos de acción alternativos.

TOTAL	SI	PARCIALMENTE	NO
24	18	5	1

Tabla 14: Resultado del análisis del proceso: Identificar soluciones automatizadas.

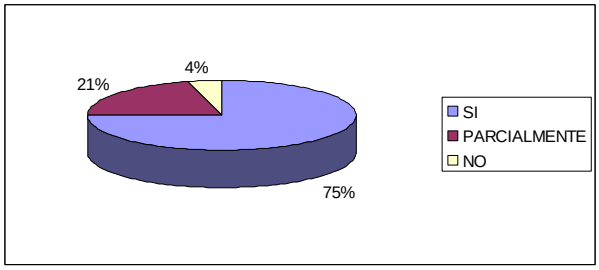


Figura 14: Estudio de factibilidad y formulación de cursos de acción alternativos.

- ***Resultados obtenidos del proceso AI2: Adquirir y mantener software aplicativo.***

Las empresas desarrolladoras de software utilizan los siguientes procesos para el desarrollo y mantenimiento del software de aplicación, que se detallan en la tabla siguiente:

PROCESO	VALOR	%
Diseño de alto nivel.	12	50
Diseño detallado.	12	50
Control y auditabilidad de las aplicaciones.	8	33
Seguridad y disponibilidad de las aplicaciones.	16	67
Configuración e implantación de software aplicativo adquirido.	11	46
Actualizaciones importantes en sistemas existentes.	13	54
Desarrollo de software aplicativo.	18	75

Aseguramiento de la Calidad del Software.	13	54
Administración de los requerimientos de aplicaciones.	16	67
Mantenimiento de software aplicativo	16	67
Otros	0	0
TOTAL		51

Tabla 15: Resultado del análisis del proceso: Adquirir y mantener software aplicativo.

- ***Resultados obtenidos por el proceso AI3: Adquirir y mantener la infraestructura tecnológica***

TOTAL	SI	PARCIALMENTE	NO
24	16	7	1

Tabla 16: Resultado del análisis del proceso: Adquirir y mantener la infraestructura tecnológica

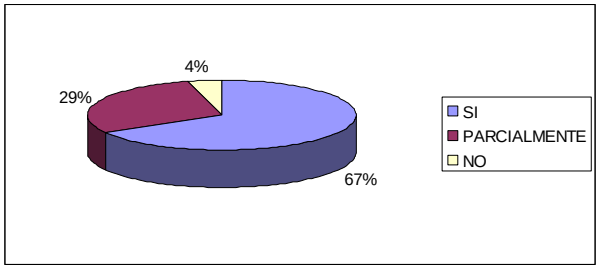


Figura 15: Adquirir y mantener la infraestructura tecnológica

- ***Resultados obtenidos por el proceso AI4: Facilitar la operación y el uso.***

Las empresas desarrolladoras de software realizan las siguientes actividades para facilitar la operación y uso de los nuevos sistemas que se detallan en la tabla siguiente:

PROCESO	VALOR	%
Desarrollar y hacer disponible la documentación de transferencia del conocimiento.	15	63
Participar y entrenar a usuarios y a la gerencia del negocio, personal de soporte y personal de operación.	18	75
Generar materiales de entrenamiento.	11	46
Otros	1	4,2
TOTAL		47

Tabla 17: Resultado del análisis del proceso: Facilitar la operación y el uso.

- ***Resultados obtenidos por el proceso AI5: Adquirir recursos de TI.***

TOTAL	SI	PARCIALMENTE	NO
24	10	12	2

Tabla 18: Resultado del análisis del proceso: Adquirir recursos de TI.

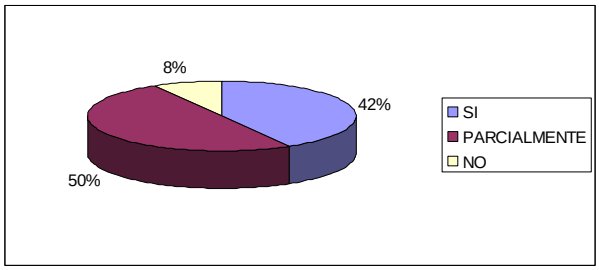


Figura 16: Adquirir recursos de TI.

- ***Resultados obtenidos por el proceso AI6: Administrar cambios***

El responsable en evaluar, priorizar y autorizar los cambios dentro del ambiente de producción en las empresas desarrolladoras de software son:

RESPONSABLE	VALOR	%
Propietario del proceso del negocio	9	38
Jefe de desarrollo	13	54
Director de administración de proyectos (PMO)	5	21
Jefe de operaciones	4	17
Otros	0	0
TOTAL		26

Tabla 19: Resultado del análisis del proceso: Administrar cambios – Responsable

Cambios de emergencia

TOTAL	FRECUENTEMENTE	AVECES	CASI NUNCA
24	6	13	5

Tabla 20: Resultado del análisis del proceso: Administrar cambios de emergencia.

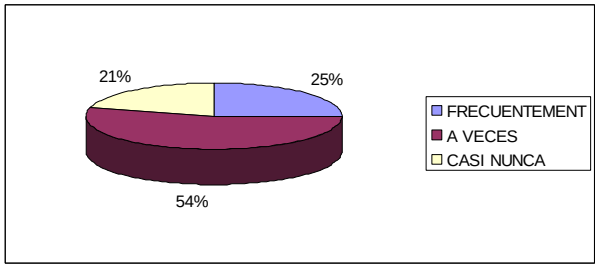


Figura 17: Cambios de emergencia.

- ***Resultados obtenidos por el proceso AI7: Instalar y acreditar soluciones y cambios.***

Ambiente de prueba

TOTAL	SI	PARCIALMENTE	NO
24	15	7	2

Tabla 21: Resultado del análisis del proceso: Ambiente de prueba

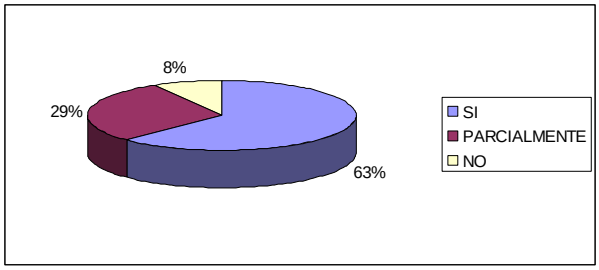


Figura 18: Ambiente de prueba.

Liberación de software

TOTAL	SI	PARCIALMENTE	NO
24	10	9	5

Tabla 22: Resultado del análisis del proceso: Liberación de software

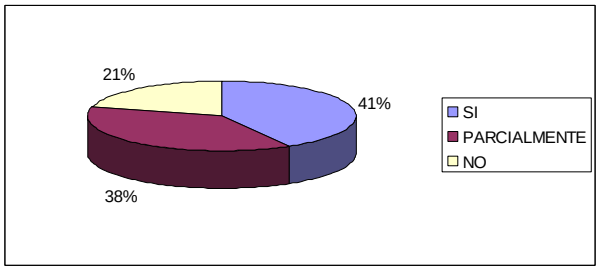


Figura 19: Liberación de software

Prueba final de aceptación.

TOTAL	SI	PARCIALMENTE	NO
24	10	12	2

Tabla 23: Resultado del análisis del proceso: Prueba final de aceptación.

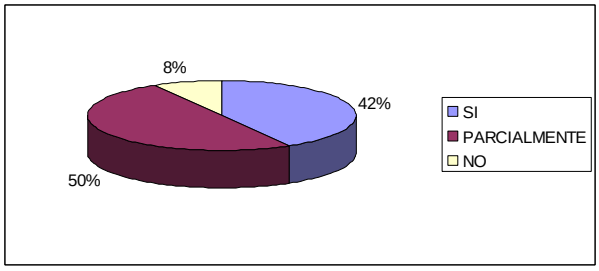


Figura 20: Prueba final de aceptación.

Revisión posterior a la implantación

TOTAL	SI	PARCIALMENTE	NO
24	17	4	3

Tabla 24: Resultado del análisis del proceso: Revisión posterior a la implantación

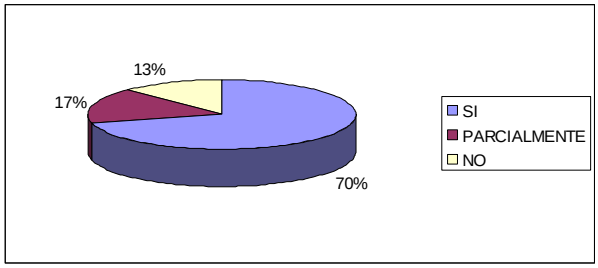


Figura 21: Revisión posterior a la implantación.

- ***Resultados obtenidos por el proceso DS1: Definir y administrar niveles de servicio.***

TOTAL	SI	PARCIALMENTE	NO
24	17	7	0

Tabla 25: Resultado del análisis del proceso: Definir y administrar niveles de servicio.

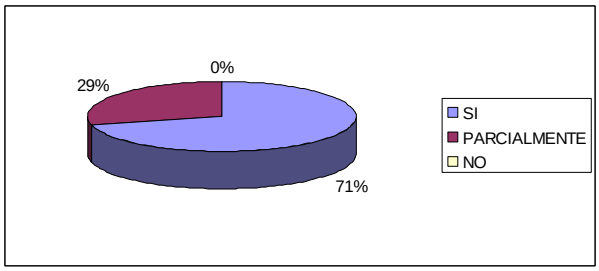


Figura 22: Definir y administrar niveles de servicio.

- ***Resultados obtenidos por el proceso DS2: Administrar servicios de terceros.***

  Identificación de las relaciones con todos los proveedores

TOTAL	SI	PARCIALMENTE	NO
24	12	11	1

Tabla 26: Resultado del análisis del proceso: Identificación de las relaciones con todos los proveedores

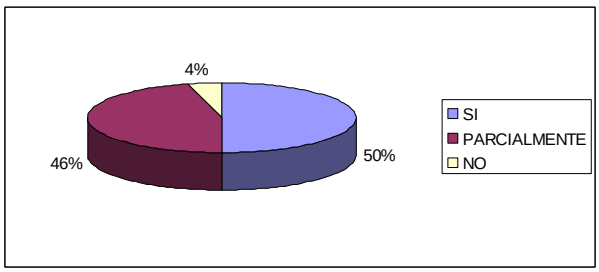


Figura 23: Identificación de las relaciones con todos los proveedores

Administración de riesgos del proveedor

TOTAL	SI	PARCIALMENTE	NO
24	9	13	2

Tabla 27: Resultado del análisis del proceso: Administración de riesgos del proveedor

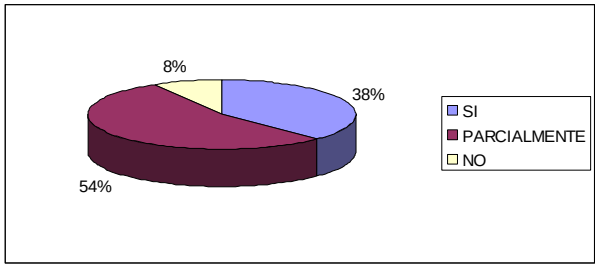


Figura 24: Identificación de las relaciones con todos los proveedores

- ***Resultados obtenidos por el proceso DS3: Administrar desempeño y capacidad.***

  Actividades que se realiza para evaluar el desempeño del sistema:

ACTIVIDADES	VALOR	%
Monitoreo del sistema.	20	83
Reporte del desempeño del sistema.	15	63
Modelado del sistema.	5	21
Pronóstico del sistema.	4	17
Otros	3	13
TOTAL		39

Tabla 28: Resultado del análisis del proceso: Administrar desempeño y capacidad – actividades.

- ***Resultados obtenidos por el proceso DS4: Garantizar la continuidad del servicio.***

  Plan de continuidad

TOTAL	SI	PARCIALMENTE	NO
24	7	9	8

Tabla 29: Resultado del análisis del proceso: Plan de continuidad.

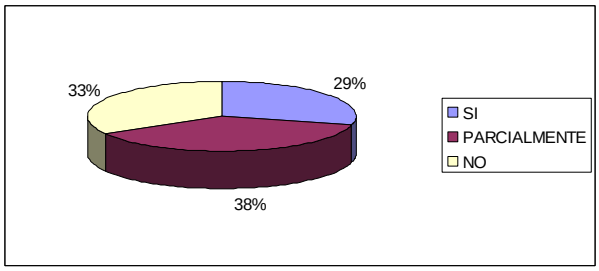


Figura 25: Plan de continuidad.

Recursos críticos de TI

TOTAL	FRECUENTEMENTE	AVECES	CASI NUNCA
24	3	2	0

Tabla 30: Resultado del análisis del proceso: Recursos críticos de TI.

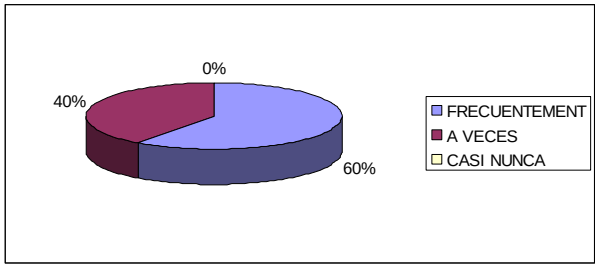


Figura 26: Recursos críticos de TI.

Actividades que se realiza con el plan de continuidad:

ACTIVIDADES	VALOR	%
Mantenimiento del plan de continuidad de TI	11	46
Pruebas del plan de continuidad de TI	14	58
Entrenamiento del plan de continuidad de TI	9	38
Distribución del plan de continuidad de TI	8	33
Otros	2	8
TOTAL		37

Tabla 31: Resultado del análisis del proceso: Actividades que se realiza con el plan de continuidad.

- ***Resultados obtenidos para el proceso DS5: Garantizar la seguridad de los sistemas***

PROCESO	VALOR	%
Administración de la seguridad de TI	12	50
Plan de seguridad de TI	8	33
Administración de identidad	11	46
Administración de cuentas del usuario	17	71
Pruebas, vigilancia y monitoreo de la seguridad	9	38
Definición de incidente de seguridad	5	21
Protección de la tecnología de seguridad	12	50
Administración de llaves criptográficas	9	38
Prevención, detección y corrección de software malicioso	15	63
Seguridad de la red	15	63
Intercambio de datos sensitivos	6	25
Otros	2	8
TOTAL		42,16

Tabla 32: Garantizar la seguridad de los sistemas

- ***Resultados obtenidos para el proceso DS6: Identificar y asignar costos***

TOTAL	SI	PARCIALMENTE	NO
24	7	7	10

Tabla 33: Resultado del análisis del proceso Identificar y asignar costos.

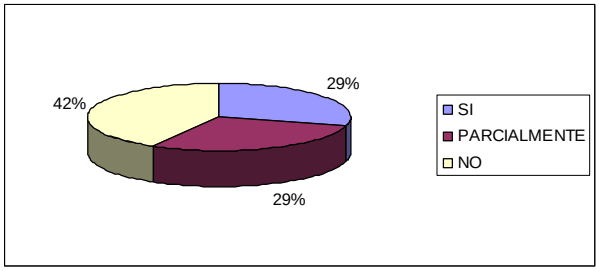


Figura 27: Identificar y asignar costos.

- ***Resultados obtenidos para el proceso DS7: Educar y entrenar a los usuarios***

TOTAL	SI	PARCIALMENTE	NO
24	11	8	5

Tabla 34: Resultado del análisis del proceso Educar y entrenar a los usuarios

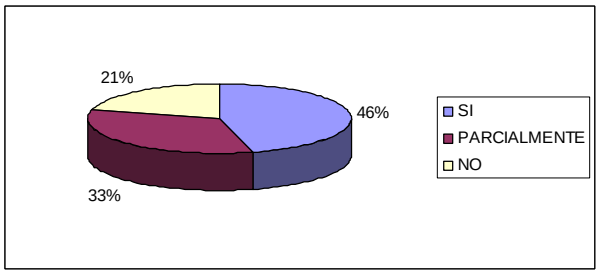


Figura 28: Educar y entrenar a los usuarios

- ***Resultados obtenidos para el proceso DS8: Administrar la mesa de servicio y los incidentes***

TOTAL	SI	PARCIALMENTE	NO
24	6	6	12

Tabla 35: Resultado del análisis del proceso Administrar la mesa de servicio y los incidentes

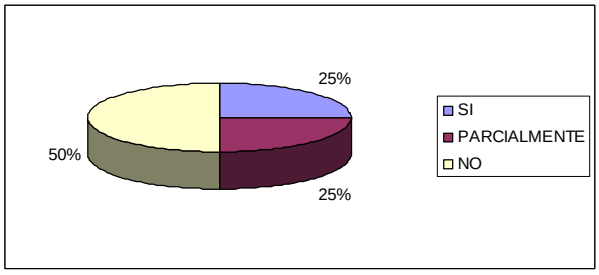


Figura 29: Administrar la mesa de servicio y los incidentes

- ***Resultados obtenidos para el proceso DS9: Administrar la configuración***

TOTAL	SI	PARCIALMENTE	NO
24	9	8	7

Tabla 36: Resultado del análisis del proceso Administrar la configuración

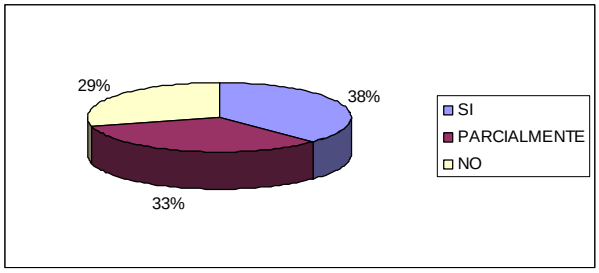


Figura 30: Administrar la configuración

- ***Resultados obtenidos para el proceso DS10: Administración de problemas***

PROCESO	VALOR	%
Identificación y clasificación de problemas	7	29
Análisis de las causas desde su raíz	5	21
Resolución de problemas	5	21
Identificación de recomendaciones para la mejora	6	25
Mantenimiento de registros de problemas	5	21
Revisión del estatus de las acciones correctivas	4	17
Otros	0	0
	TOTAL	16

Tabla 37: Resultado del análisis del proceso Administración de problemas

- ***Resultados obtenidos para el proceso DS11: Administración de la Información***

Administración de datos

TOTAL	SI	PARCIALMENTE	NO
24	15	9	0

Tabla 38: Resultado del análisis del proceso Requerimientos del negocio para administración de datos

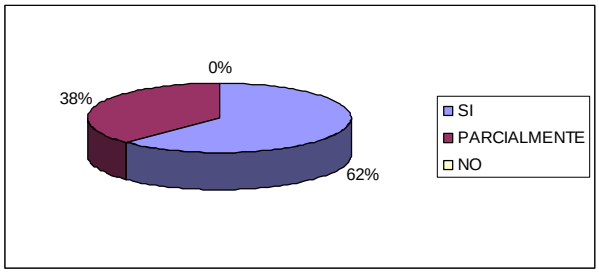


Figura 31: Requerimientos del negocio para administración de datos

Acuerdos de almacenamiento y conservación

TOTAL	SI	PARCIALMENTE	NO
24	16	5	3

Tabla 39: Resultado del análisis del proceso Acuerdos de almacenamiento y conservación

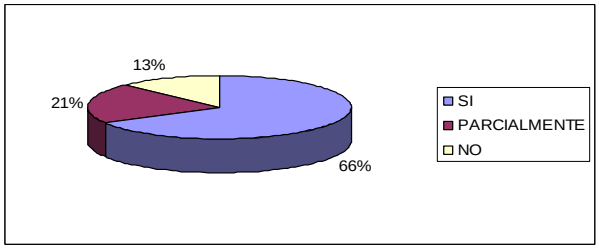


Figura 32: Acuerdos de almacenamiento y conservación

Respaldo y restauración

TOTAL	SI	PARCIALMENTE	NO
24	15	6	3

Tabla 40: Resultado del análisis del proceso Respaldo y restauración

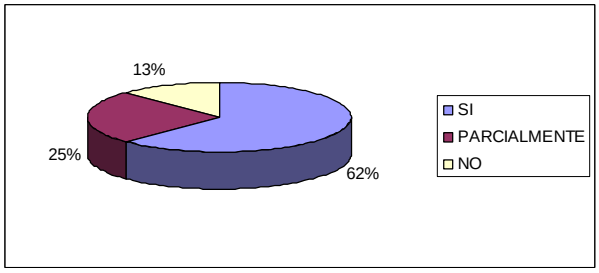


Figura 33: Respaldo y restauración

- ***Resultados obtenidos para el proceso DS12: Administración del ambiente físico.***

Medidas de seguridad física

TOTAL	SI	PARCIALMENTE	NO
24	13	9	2

Tabla 41: Resultado del análisis del proceso Medidas de seguridad física

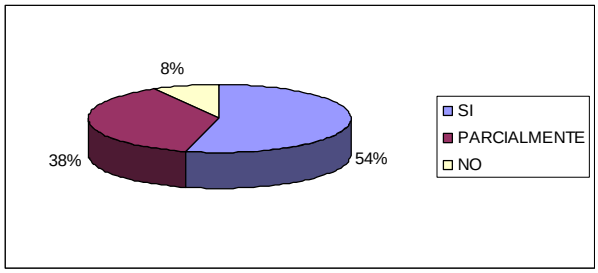


Figura 34: Medidas de seguridad física

Protección contra factores ambientales.

TOTAL	SI	PARCIALMENTE	NO
24	5	7	12

Tabla 42: Resultado del análisis del proceso Protección contra factores ambientales.

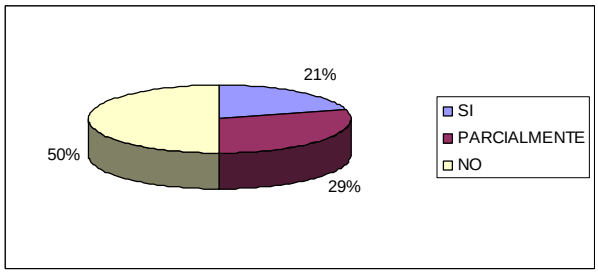


Figura 35: Protección contra factores ambientales.

- ***Resultados obtenidos para el proceso DS13: Administración de Operaciones***

TOTAL	SI	PARCIALMENTE	NO
24	13	11	0

Tabla 43: Resultado del análisis del proceso Administración de Operaciones

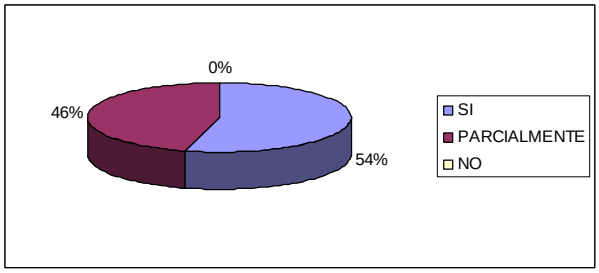


Figura 36: Administración de Operaciones

- ***Resultados obtenidos para el proceso ME1: Monitorear y evaluar el desempeño de TI.***

Definición y recolección de Datos de Monitoreo

TOTAL	SI	PARCIALMENTE	NO
24	12	7	5

Tabla 44: Resultado del análisis del proceso Definición y recolección de Datos de Monitoreo

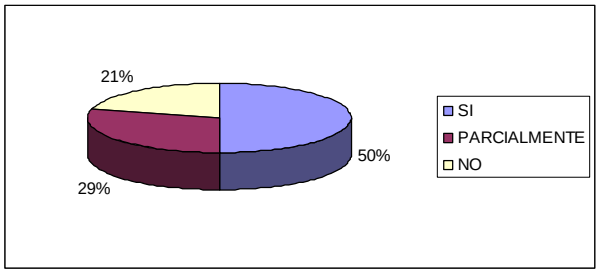


Figura 37: Definición y recolección de Datos de Monitoreo

Evaluación del Desempeño

TOTAL	SI	PARCIALMENTE	NO
24	8	7	9

Tabla 45: Resultado del análisis del proceso Evaluacion del Desempeño

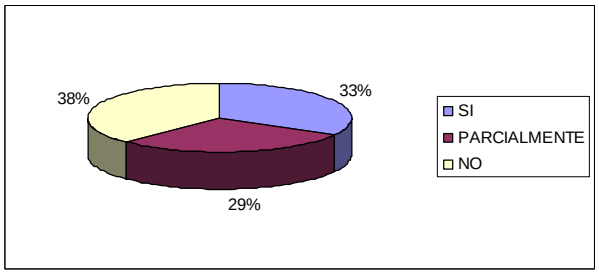


Figura 38: Evaluacion del Desempeño

Reportes al consejo directivo y a ejecutivos.

TOTAL	SI	PARCIALMENTE	NO
24	8	8	8

Tabla 46: Resultado del análisis del proceso Reportes al consejo directivo y a ejecutivos.

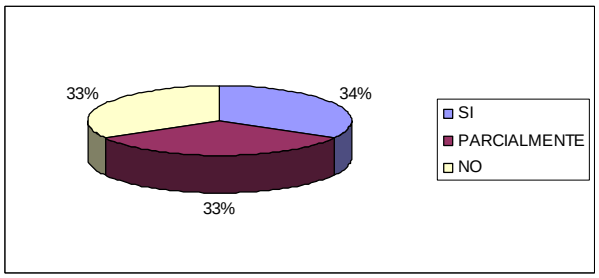


Figura 39: Reportes al consejo directivo y a ejecutivos.

Acciones Correctivas

TOTAL	SI	PARCIALMENTE	NO
24	17	1	6

Tabla 47: Resultado del análisis del proceso Acciones Correctivas

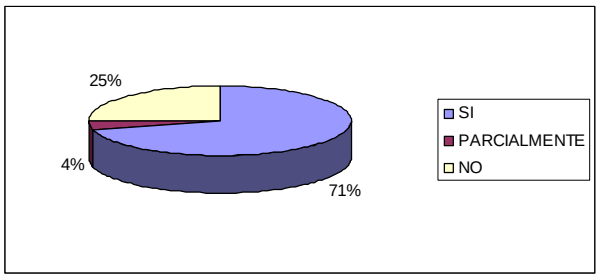


Figura 40: Acciones Correctivas

- ***Resultados obtenidos para el proceso ME2: Monitorear y evaluar el control interno.***

Monitorear el marco de trabajo de control interno

TOTAL	SI	PARCIALMENTE	NO
24	12	7	5

Tabla 48: Resultado del análisis del proceso Monitorear el marco de trabajo de control interno

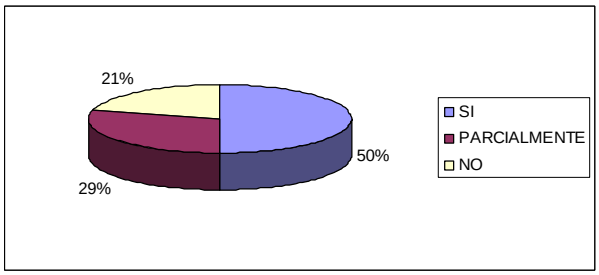


Figura 41: Monitorear el marco de trabajo de control interno

Aseguramiento del control interno

TOTAL	SI	PARCIALMENTE	NO
24	12	9	3

Tabla 49: Resultado del análisis del proceso Aseguramiento del control interno

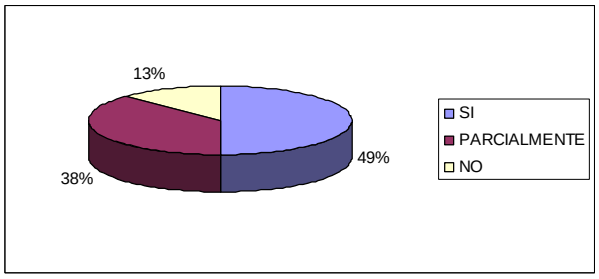


Figura 42: Aseguramiento del control interno

Acciones correctivas

TOTAL	SI	PARCIALMENTE	NO
24	13	9	2

Tabla 50: Resultado del análisis del proceso Acciones correctivas

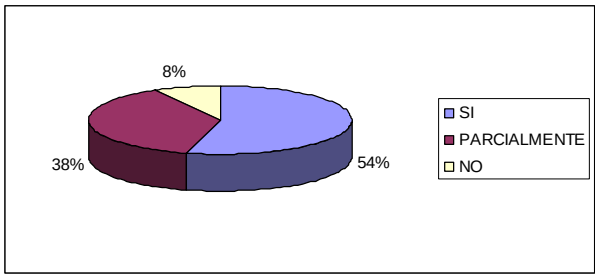


Figura 43: Acciones correctivas

- ***Resultados obtenidos para el proceso ME3: Garantizar el cumplimiento regulatorio.***

PROCESO	**VALOR**	**%**
Identificar los requisitos legales y regulatorios con TI	6	25
Entrenar al personal de TI sobre su responsabilidad de cumplimiento	5	21
Evaluar el impacto de los requisitos regulatorios.	6	25
Monitorear y reportar el cumplimiento de los requerimientos regulatorios	4	17
Otros	1	4
TOTAL		18

Figura 44: Garantizar el cumplimiento regulatorio

- ***Resultados obtenidos para el proceso ME4: proporcionar Gobierno de TI.***

Establecer un marco de trabajo de gobierno para TI

TOTAL	SI	PARCIALMENTE	NO
24	9	4	11

Tabla 51: Resultado del análisis del proceso Establecer un marco de trabajo de gobierno para TI

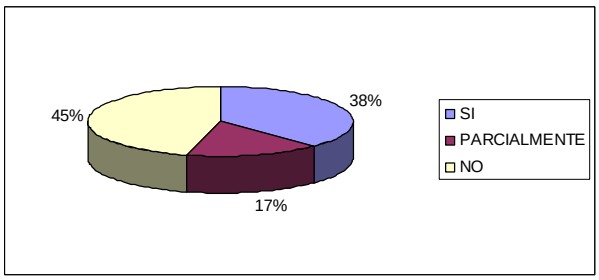


Figura 45: Establecer un marco de trabajo de gobierno para TI

Alineamiento estratégico

TOTAL	SI	PARCIALMENTE	NO
24	8	7	9

Tabla 52: Resultado del análisis del proceso Alineamiento estratégico

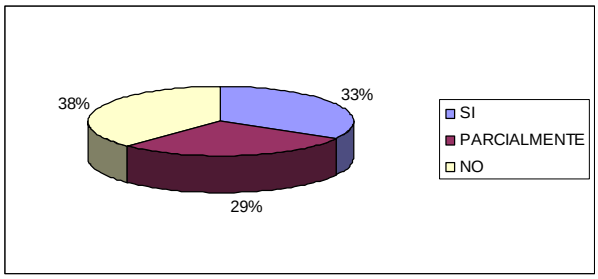


Figura 46: Alineamiento estratégico

Administración de Riesgos

TOTAL	SI	PARCIALMENTE	NO
24	8	8	8

Tabla 53: Resultado del análisis del proceso Administración de Riesgos

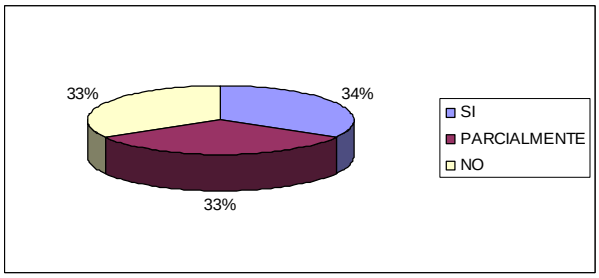


Figura 47: Administración de Riesgos

Medición del Desempeño

TOTAL	SI	PARCIALMENTE	NO
24	11	4	9

Tabla 54: Resultado del análisis del proceso Medición del Desempeño

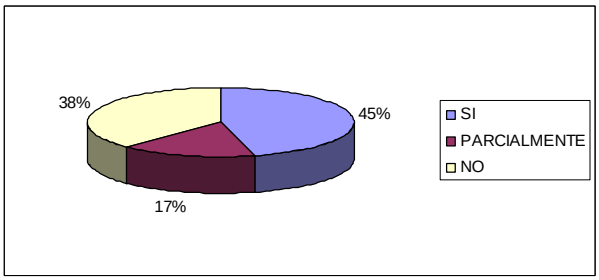


Figura 48: Medición del Desempeño

Aseguramiento Independiente

TOTAL	SI	PARCIALMENTE	NO
24	14	5	5

Tabla 55: Resultado del análisis del proceso Aseguramiento Independiente

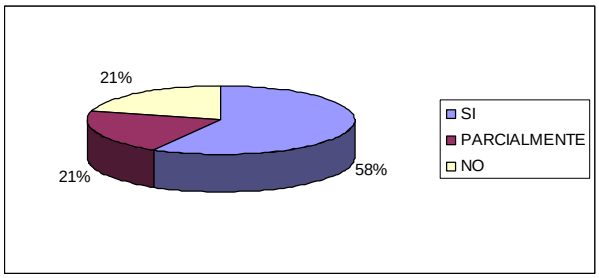


Figura 49: Aseguramiento Independiente

2.3.2.2 Análisis de los resultados obtenidos

Luego de tabular los datos de los resultados obtenidos de las encuestas realizadas, se procede a realizar el análisis de resultados para lo cual se tomara como referencia el cuadro de interpretación conforme lo sugiere COSO Sponsoring Organizations of the Treadway Commission (VER ANEXO 3).

Cada uno de los procesos del COBIT 4.0 están ordenados ascendentemente de acuerdo a los índices de confianza y de riesgo propuesto por COSO.

DS10: Administración de problemas

Según los resultados obtenidos se ha determinado que el grado de confianza que tiene este proceso es bajo (B) y el nivel de riesgo es alto (A). Por consiguiente será tomado en cuenta para la formulación de un proceso para evaluar el desempeño de las empresas desarrolladoras de software, en cuanto a las operaciones de TI utilizando COBIT 4.0.

ME3: Garantizar el cumplimiento regulatorio.

En base a los resultados de las encuestas, el grado de confianza que tiene este proceso es bajo (B) y el nivel de riesgo es alto (A). Así y de acuerdo a los indicadores será tomado en cuenta en la elaboración del proceso.

DS8: Administrar la mesa de servicio y los incidentes

Analizando los resultados de la encuesta referentes a este proceso, el grado de confianza que tiene el mismo es bajo (B) y el nivel de riesgo es alto (A). Por consiguiente y basándonos en los indicadores será tomado en cuenta para el desarrollo del proceso.

AI6: Administrar cambios.

Las encuestas realizadas en las empresas que son objeto de nuestro estudio tienen un grado de confianza bajo (B) y el nivel de riesgo es alto (A), en consecuencia se ha establecido que formará parte del proceso de evaluación de las operaciones de TI.

DS6: Identificar y asignar costos

Según la información obtenida se pudo concluir que, el grado de confianza que tiene este proceso es bajo (B) y el nivel de riesgo es alto (A). En base a estos indicadores se aplicará en el desarrollo del proceso.

DS12: Administración del ambiente físico.

El grado de confianza que toma el proceso es bajo (B) y el nivel de riesgo es alto (A). Haciendo referencia a estos indicadores se lo aplicará en la elaboración del proceso.

DS9: **Administrar la configuración**

En referencia a este proceso y de acuerdo a los resultados obtenidos en la encuesta, el grado de confianza asignado al mismo es moderado (M) y el nivel de riesgo es moderado (M). En base a estos indicadores se lo aplicará en el desarrollo del proceso.

PO10: Administrar proyectos.

Acorde a los resultados obtenidos se puede precisar que el grado de confianza es moderado (M) y el nivel de riesgo que tiene este proceso es moderado (M), en consecuencia se ha establecido que será parte de la elaboración del proceso.

DS3: Administrar desempeño y capacidad.

El grado de confianza que tiene este proceso es moderado (M) y el nivel de riesgo también es moderado (M), por lo tanto se ha determinado que se usará para el desarrollo del proceso de evaluación de las operaciones de TI de las empresas desarrolladoras de software.

ME4: Proporcionar Gobierno de TI.

Acorde a los resultados obtenidos se puede precisar que el grado de confianza es moderado (M) y el nivel de riesgo que tiene este proceso es moderado (M), así y de acuerdo a los indicadores será tomado en cuenta en la elaboración del proceso.

DS4: Garantizar la continuidad del servicio.

Según las encuestas realizadas se obtiene que este proceso tiene un grado de confiabilidad moderado (M) y el nivel de riesgo moderado (M), consecuentemente se ha determinado que serán tomados en consideración para la formulación del proceso.

DS5: Garantizar la seguridad de los sistemas

De acuerdo a los resultados obtenidos, el grado de confianza que tiene este proceso es moderado (M) y el nivel de riesgo es moderado (M). Concluyendo que se lo aplicará en la elaboración del proceso.

PO7: Administrar recursos humanos de TI.

En las empresas que han sido objeto de nuestro estudio el grado de confianza que tiene este proceso es moderado (M) y el nivel de riesgo es moderado (M), consecuentemente se ha acordado que será parte del proceso a desarrollar.

DS2: Administrar servicios de terceros.

Acorde a los resultados obtenidos se obtiene un grado de confianza moderado (M) y el nivel de riesgo también es moderado (M), en consecuencia se usará para la formulación del proceso.

DS7: Educar y entrenar a los usuarios

El grado de confianza que tiene este proceso es moderado (M) y el nivel de riesgo es moderado (M). Así en base en los indicadores anteriores se lo tomara en cuenta para la formulación del proceso.

AI4: Facilitar la operación y el uso.

Utilizando el cuadro de interpretación del COSO sabemos que el grado de confianza que tiene este proceso es moderado (M) y el nivel de riesgo es moderado (M), por consiguiente se ha acordado que se aplicará para la elaboración del proceso.

ME1: Monitorear y evaluar el desempeño de TI.

Según los resultados obtenidos este proceso tiene un grado de confianza moderado (M) y un nivel de riesgo moderado (M). Analizando los indicadores será tomado en cuenta para la elaboración del proceso.

AI5: Adquirir recursos de TI.

Se ha estipulado mediante las encuestas que hay un grado de confianza moderado (M) y el nivel de riesgo es moderado (M). Por consiguiente se ha establecido que será parte del proceso para analizar el entorno de trabajo actual de las empresas desarrolladoras de software.

AI2: Adquirir y mantener el software aplicativo.

Mediante el resultado de las encuestas se ha precisado que tienen un grado de confianza moderado (M) y el nivel de riesgo es moderado (M), por consiguiente se ha determinado que formará parte de la elaboración del proceso.

ME2: Monitorear y evaluar el control interno.

De acuerdo a los resultados de las encuestas se obtiene un grado de confianza moderado (M) y un nivel de riesgo moderado (M). Haciendo referencia a estos indicadores se aplicará en la elaboración del proceso.

AI7: Instalar y acreditar soluciones y cambios.

Según las encuestas realizadas se ha determinado que este proceso tiene un grado de confianza moderado (M) y el nivel de riesgo también es moderado (M), en consecuencia se usará para el desarrollo del proceso.

DS13: Administración de Operaciones

En lo que respecta a este proceso y de acuerdo a resultados de la encuesta, el grado de confianza que tiene es moderado (M) y el nivel de riesgo es moderado (M). En base a estos indicadores se aplicará en la formulación del proceso.

PO5: Administrar la inversión en TI.

Se ha estipulado mediante las encuestas que hay un grado de confianza moderado (M) y el nivel de riesgo es moderado (M). Por consiguiente se ha establecido que será parte del proceso para analizar el entorno de trabajo actual de las empresas.

PO9: Evaluar y administrar riesgos de TI

De conformidad con los resultados de las encuestas se ha determinado que el grado de confianza es moderado (M) y el nivel de riesgo que tiene este proceso es moderado (M), por lo tanto se ha decidido que será parte del proceso.

PO1: Definir un plan estratégico para TI

Se ha determinado que el plan estratégico de TI de las empresas desarrolladoras de software tiene un grado de confianza moderado (M) y el nivel de riesgo es moderado (M). Por consiguiente será tomado en cuenta para la formulación del proceso.

PO6: Comunicar las aspiraciones y la dirección de la gerencia.

Utilizando el cuadro de interpretación del COSO sabemos que el grado de confianza que tiene este proceso es moderado (M) y el nivel de riesgo es moderado (M), por consiguiente se ha acordado que se aplicará para la elaboración del proceso.

DS11: Administración de la Información

En lo que respecta a requerimientos del negocio para administración de datos, en las empresas desarrolladoras de software se tiene un grado de confianza moderado (M) y un nivel de riesgo moderado (M). Basándonos en estos indicadores se lo aplicará en la elaboración del proceso.

PO8: Administrar calidad.

Se ha determinado que el grado de confianza que obtiene este proceso es moderado (M) y el nivel de riesgo es moderado (M), por ende será parte de la elaboración del proceso para evaluar el desempeño de las operaciones de TI.

AI3: Adquirir y mantener la infraestructura tecnológica

De acuerdo a los resultados obtenidos se ha determinado que el uso de las plataformas apropiadas para soportar las aplicaciones del negocio tienen un grado de confianza

moderado (M) y el nivel de riesgo es moderado (M), por ende se ha establecido que formará parte de la elaboración del proceso.

PO2: Definir la arquitectura de la información

Según las respuestas de las encuestas se ha precisado que tiene un grado de confianza moderado (M) y el nivel de riesgo es moderado (M), por ende se aplicará para el desarrollo del proceso para analizar el entorno de trabajo actual de las empresas desarrolladoras de software.

DS1: Definir y administrar niveles de servicio.

Conforme a los resultados obtenidos, se ha determinado que el grado de confianza es alto (A) y que el nivel de riesgo es bajo (B), en consecuencia no se aplicará para el desarrollo del proceso.

AI1: Identificar soluciones automatizadas.

De acuerdo al cuadro de interpretación del COSO se ha determinado que las definiciones de las necesidades técnicas y funcionales del negocio, tienen un grado de confianza alto (A) y que el nivel de riesgo es bajo (B), en consecuencia no se aplicará para el desarrollo del proceso.

PO4: Definir procesos, organización y relaciones de TI.

El grado de confianza que tiene este proceso es alto (A) y el nivel de riesgo es bajo (B). Subsiguientemente se ha establecido que no se aplicará en la formulación del proceso de evaluación del desempeño a las empresas desarrollo de software.

PO3: Determinar la dirección tecnológica.

Manejando el cuadro de interpretación del COSO sabemos que el grado de confianza que tiene este proceso es alto (A) y el nivel de riesgo es bajo (B). Por lo tanto se ha determinado que no se aplicará en el desarrollo del proceso de evaluación.

2.3.2.3 Análisis resultados vs. Importancia procesos COBIT 4.0.

En base al análisis de los resultados obtenidos que se encuentran en la sección 2.3.2.2, y al nivel de importancia de los procesos del COBIT 4.0, se debe tomar en cuenta lo siguiente:

- Si la interpretación es **Baja** se entenderá que es absolutamente necesario tomar medidas inmediatas a fin de evitar problemas y mejorar el aspecto auditado, poniendo gran énfasis en los criterios con bajo puntaje.
- Si la interpretación es **Media** se entenderá que es siempre posible mejorar los criterios donde no se ha conseguido un elevado puntaje y que las medidas no son tan inmediatas como el caso anterior. Hay que tomar en cuenta los criterios con alto puntaje de manera que se mantengan en ese estado.
- Si la interpretación es **Alta** se entenderá que la gestión del aspecto auditado se esta llevando de manera adecuada y que es preciso mantenerlo de esa forma.

PROCESOS DE COBIT	RESULTADOS ANÁLISIS	RESULTADOS
PO2	DS10	Importancia del proceso **PO2** = baja, **DS10:** Grado de confianza = bajo, Nivel de riesgo = alto. **Se aplicará a la formulación del proceso**
PO4	ME3	Importancia del proceso **PO4** = baja, **ME3:** Grado de confianza = bajo , nivel de riesgo = alto. **Se aplicará a la formulación del proceso**
PO7	DS8	Importancia del proceso **PO7** = baja, **DS8:** Grado de confianza = bajo , Nivel de riesgo = alto. **Se aplicará a la formulación del proceso**
AI3	AI6	Importancia del proceso **AI3**= baja, **AI6:** Grado de confianza = bajo , Nivel de riesgo = alto. **Se aplicará a la formulación del proceso**
AI4	DS6	Importancia del proceso **AI4** = baja, **DS6:** Grado de confianza = bajo , Nivel de riesgo = alto.

		Se aplicará a la formulación del proceso
DS2	DS12	Importancia del proceso **DS2** = baja, **DS12:** Grado de confianza = bajo , Nivel de riesgo = alto. **Se aplicará a la formulación del proceso**
DS3	DS9	Importancia del proceso **DS3** = baja, **DS9:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
DS6	PO10	Importancia del proceso **DS6** = baja, **PO10:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
DS7	DS3	Importancia del proceso **DS7** = baja, **DS3:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
DS8	ME4	Importancia del proceso **DS8** = baja, **ME4:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
DS12	DS4	Importancia del proceso **DS12**= baja, **DS4:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
DS13	DS5	Importancia del proceso **DS13** = baja, **DS5:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
PO3	PO7	Importancia del proceso **PO3** = media, **PO7:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
PO5	DS2	Importancia del proceso **PO5** = media, **DS2:** Grado de confianza = moderado,

		Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
PO6	DS7	Importancia del proceso **PO6** = media, **DS7:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
PO8	AI4	Importancia del proceso **PO8** = media, **AI4:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
AI1	ME1	Importancia del proceso **AI1** = media, **ME1:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
AI2	AI5	Importancia del proceso **AI2** = media, **AI5:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
AI5	AI2	Importancia del proceso **AI5** = media, **AI2:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
AI7	ME2	Importancia del proceso **AI7** = media, **ME2:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
DS1	AI7	Importancia del proceso **DS1** = media, **AI7:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
DS4	DS13	Importancia del proceso **DS4** = media, **DS13:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
DS9	PO5	Importancia del proceso **DS9** = media,

		PO5: Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
DS10	PO9	Importancia del proceso **DS10**= media, **PO9:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
ME2	PO1	Importancia del proceso **ME2** = media, **PO1:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
PO1	PO6	Importancia del proceso **PO1** = alta, **PO6:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
PO9	DS11	Importancia del proceso **PO9** = alta, **DS11:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
PO10	PO8	Importancia del proceso **PO10** = alta, **PO8:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
AI6	AI3	Importancia del proceso **AI6** = alta, **AI3:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
DS5	PO2	Importancia del proceso **DS5** = alta, **PO2:** Grado de confianza = moderado, Nivel de riesgo = moderado. **Se aplicará a la formulación del proceso**
DS11	DS1	Importancia del proceso **DS11 =** alta, **DS1:** Grado de confianza = alto, Nivel de riesgo = bajo. **No se aplicará a la formulación del proceso**

ME1	AI1	Importancia del proceso **ME1** = alta, **AI1:** Grado de confianza = alto, Nivel de riesgo = bajo. **No se aplicará a la formulación del proceso**
ME3	PO4	Importancia del proceso **ME3** = alta, **PO4:** Grado de confianza = alto, Nivel de riesgo = bajo. **No se aplicará a la formulación del proceso**
ME4	PO3	Importancia del proceso **ME4** = alta, **PO3:** Grado de confianza = alto, Nivel de riesgo = bajo. **No se aplicará a la formulación del proceso**

Tabla 56: Análisis resultados vs. Importancia Procesos COBIT 4.0.

CAPÍTULO 3: FORMULACIÓN DEL PROCESO

3.1 ALCANCE Y OBJETIVOS DEL PROCESO

3.1.1 ALCANCE DEL PROCESO

El proceso pretende convertirse en un marco de referencia, para la evaluación de las operaciones de TI, específicamente para empresas desarrolladoras de software en base a la metodología COBIT 4.0, acorde a su situación actual.

El proceso que se va desarrollar se espera que sea de mucha utilidad para las empresas dedicadas al desarrollo de software ya que contemplará procedimientos claves para alcanzar calidad en sus procesos.

La elaboración del proceso está enfocada para el uso de los administradores de las operaciones de TI, así como también para los auditores informáticos de las empresas desarrolladoras de software. Con el fin apoyar en el desenvolvimiento de los mismos se presenta un caso práctico.

Las empresas que deseen implantar este proceso deberán tener conocimientos previos de COBIT 4.0 para poder aplicarla de manera óptima.

3.1.2 OBJETIVO DEL PROCESO

Para realizar este proceso se plantean los siguientes objetivos:

- Facilitar a las empresas desarrolladoras de software un proceso que les permita evaluar sus operaciones de TI.
- Mejorar el rendimiento de los Administradores de TI, presentado un conjunto de pasos metódicos para el gobierno de TI, en base a COBIT 4.0. ya que se reducirá los procesos del mismo ajustándose solo a dichas empresas, y facilitando las tareas de los Administradores de las operaciones de TI.
- Aplicar el proceso propuesto en una empresa desarrolladora de software para validarlo.

3.1.3 ¿A QUIÉN ESTA DIRIGIDA?

Aunque un conocimiento en profundidad de las técnicas y herramientas para evaluar las operaciones de TI de las empresas desarrolladoras de software, puede estar reservado a los profesionales de la materia, nuestro propósito al realizar este trabajo ha sido dirigido a una audiencia mucha más amplia que comprende:

Ejecutivos

Son los responsables de la gestión, adquisición y utilización de los recursos de TI de la organización.

Por lo tanto deben velar por los intereses de la empresa, evitando problemas legales y de negocios, administrando la parte económica e implementando procedimientos de control sobre las TI.

Auditores

Este proceso permitirá a los auditores dar valor agregado a su gestión informática, utilizando nuevos y ampliados conocimientos con relación al estándar utilizado para el desarrollo del mismo (COBIT 4.0).

Administradores de TI

El proceso mejorar el rendimiento de los Administradores de TI, presentado un conjunto de pasos metódicos para el gobierno de TI, en base a COBIT 4.0.

Estudiantes Universitarios

Este proceso servirá como un documento de consulta para los estudiantes que requieren algún tipo de información sobre este tema, lo que permitirá ampliar sus conocimientos.

3.2 FORMULACIÓN DEL PROCESO

3.2.1 PLANEAR Y ORGANIZAR

Este dominio cubre la estrategia y las tácticas y corresponde a la identificación de la forma en que la información tecnológica puede contribuir de mejor manera a alcanzar a los objetivos de gestión.

3.2.1.1 PO1: Definir un plan estratégico para TI

Alcanzar un equilibrio óptimo de oportunidades de tecnología de la información y de los requerimientos de TI del negocio así como también asegurar su cumplimiento posterior. Es posibilitado por un proceso de planeación estratégica, promovido a intervalos regulares dando lugar a planes a largo plazo, los mismos que deben ser traducidos periódicamente en planes operativos, que fijan a corto plazo metas claras y concretas.

Criterios a considerar para el cumplimiento de este proceso:

- Tener definido un plan estratégico de TI y que este se encuentre alineado con las necesidades del negocio.
- Realizar la evaluación del desempeño de los planes existentes y de los sistemas de información.
- Traducir el plan estratégico de TI a planes tácticos.
- Analizar portafolios de programas y administrar portafolios de servicios y proyectos.

3.2.1.2 PO2: Definir la arquitectura de la información

Mejorar la organización de los sistemas de información, se lo logra mediante la creación y el mantenimiento de un modelo de información de negocios y asegurando que estén definidos los sistemas adecuados para optimizar el uso de esta información.

Criterios a considerar para el cumplimiento de este proceso:

- Tiene definida la arquitectura de la información.
- Cuenta con un diccionario de datos empresarial.

3.2.1.3 PO5: Administrar la inversión en TI

Asegurar el financiamiento y el control de desembolsos de recursos financieros. Es posibilitado por medio de una inversión periódica y de un presupuesto operativo establecido y aprobado por el negocio.

Criterios a considerar para el cumplimiento de este proceso:

- Establece un marco de trabajo financiero para TI que impulse el presupuesto y el análisis de rentabilidad, con base en los portafolios de inversión, servicios y activos.
- Se implanta un proceso de toma de decisiones para dar prioridades a la asignación de recursos de TI.

- Establece y mantiene un proceso presupuestal de TI.
- Implanta un proceso de administración de costos que compare los costos reales con los presupuestados.
- Implanta un proceso de monitoreo de beneficios

3.2.1.4 PO6: Comunicar las aspiraciones y la dirección de la gerencia

Asegurar el conocimiento y la comprensión del personal, de los objetivos de alto nivel (gerencia), se lo logra a través de políticas establecidas y comunicadas al personal; por otra parte, es necesario establecer normas para traducir las opciones estratégicas en reglas prácticas y utilizables por el personal.

Criterios a considerar para el cumplimiento de este proceso:

- Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa.
- Elaborar y dar mantenimiento a un marco de trabajo enfocado en los riesgos y control interno, para entregar valor mientras al mismo tiempo se protegen los recursos y sistemas de TI.
- Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI.
- Implantar y comunicar las políticas de TI al personal que le compete.
- Asegurar que la conciencia y el entendimiento de los objetivos de la dirección del negocio y de TI. se comunican a toda la organización.

3.2.1.5 PO7: Administrar los recursos humanos de TI

Adquirir y mantener una fuerza de trabajo motivada y competente y maximizar las contribuciones del personal a los procesos de TI. Es facilitado por prácticas sanas, justas y transparentes de administración de personal para reclutar, contratar, pensionar, compensar, entrenar, evaluar, promover así como despedir.

Criterios a considerar para el cumplimiento de este proceso:

- Asegurar que el reclutamiento del personal de TI. se lleve a cabo de acuerdo a políticas y procedimientos generales de personal de la organización.
- Verificar periódicamente que el personal este capacitado.

- Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal en base a políticas administrativas.
- Capacitar constantemente al personal de TI.
- Minimizar el grado de dependencia del personal indispensable.
- Minimizar el riesgo del cambio de puesto o terminación del trabajo del personal.

3.2.1.6 PO8: Administrar la calidad

Satisfacer los requerimientos de clientes de TI. Es posibilitado por la planificación, implementación y mantenimiento de normas y sistemas de administración de calidad proporcionando fases distintas de desarrollo, productos claros y responsabilidades explícitas.

Criterios a considerar para el cumplimiento de este proceso:

- Monitorear y medir la efectividad y aceptación del QMS y mejorarlo cuando sea necesario.
- Identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI. para orientar a la organización hacia el cumplimiento del QMS.
- Adoptar y mantener estándares para todo el desarrollo y adquisición que sigue el ciclo de vida hasta el último entregable.
- Garantizar que la administración de calidad se enfoquen los clientes, determine sus requerimientos y los alinee con los estándares y prácticas de TI.
- Elaborar y comunicar un plan global de calidad que promueva la mejora continua, de forma periódica.
- Definir, planear e implementar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que este proporciona.

3.2.1.7 PO9: Evaluar y administrar los riesgos de TI

Apoyar las decisiones de la administración para lograr los objetivos de TI y responder a las amenazas reduciendo la complejidad, la objetividad creciente e identificando factores importantes de decisión. Para ello se logra la participación de la propia organización en la identificación de riesgos y al análisis de impactos de TI, que involucran funciones multidisciplinarias y tomando medidas de eficiencia de costos para mitigar los riesgos.

Criterios a considerar para el cumplimiento de este proceso:

- Integrar el gobierno, la administración de riesgos y el marco de control de TI al marco de trabajo de administración de riesgos de la organización.
- Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados.
- Identificar las amenazas y vulnerabilidades que afectan al normal desempeño de la empresa.
- Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos.
- Elaborar y mantener respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continua.
- Asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarios, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución.

3.2.1.8 PO10: Administrar Proyectos

Establecer prioridades y entregar servicios oportunamente y dentro del presupuesto. Es posibilitado por la organización que identifica y da prioridad a los proyectos en línea con el plan operativo y la adopción y aplicación de técnicas saludables de administración de proyectos para cada proyecto emprendido.

Criterios a considerar para el cumplimiento de este proceso:

- Mantener el programa de los proyectos, relacionados con el portafolio de los programas de inversión en TI.
- Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas.
- Establecer un enfoque de administración de proyectos que corresponda al tamaño complejidad y requerimientos regulatorios de cada proyecto.
- Asegurar que todos los proyectos de TI cuenten con patrocinadores con la suficiente autoridad para apropiarse de la ejecución del proyecto dentro del programa estratégico global.

- Obtener el compromiso y participación de los interesados afectados en la definición y ejecución del proyecto dentro del contexto del programa global de inversión en TI.
- Definir y documentar la naturaleza y alcance del proyecto para conformar y desarrollar, entre los interesados, un entendimiento común del alcance del proyecto y su relación con otros proyectos dentro del programa global de inversiones en TI.
- Asegurar que el arranque de las etapas importantes del proyecto se aprueben de manera formal y se comunique a todos los interesados.
- Establecer un plan integrado para el proyecto, aprobado y formal para guiar la ejecución y control del proyecto a lo largo de la vida de este.
- Entender y documentar dentro de un mismo programa las actividades e interdependencias de múltiples proyectos.
- Definir las responsabilidades, relaciones, autoridades y criterios de desempeño de los miembros del equipo del proyecto y especifica las bases para adquirir y asignar a los miembros competentes del equipo y/o los contratistas al proyecto.
- Eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, análisis, respuesta, monitoreo y control de las áreas o eventos que tenga el potencial de ocasionar cambios no deseados.
- Preparar un plan de administración de la calidad que describa el sistema de calidad del proyecto y como será implantado.
- Revisar y acuerda el plan de calidad de proyecto con todas las partes interesadas para luego ser incorporado en el plan integrado del proyecto.
- Establecer un sistema de control de cambios para cada proyecto, de tal modo que todos los cambios a la línea base del proyecto se revisen, aprueben e incorporen de manera apropiada al plan integrado del proyecto, de acuerdo al marco de trabajo del gobierno del programa y del proyecto.
- Identificar las tareas de aseguramiento requeridas para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado.
- Medir el desempeño del proyecto contra los criterios claves del proyecto y recomienda, implanta y monitorea las medidas correctivas según sea requerido, de acuerdo con el marco de trabajo de gobierno del programa y del proyecto.

- Solicitar que al finalizar cada proyecto, los interesados del proyecto se cercioren de que el proyecto haya cubierto los resultados y beneficios esperados.

3.2.2 ADQUIRIR E IMPLANTAR

Para llevar a cabo las estrategias de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además este dominio cubre los cambios y el mantenimiento realizado a los sistemas existentes.

3.2.2.1 AI2: Adquirir y mantener software aplicativo

Proporciona funciones automatizadas que soporten efectivamente el proceso del negocio a través de la definición de las declaraciones específicas de requerimientos funcionales y operativos, y una implementación estructurada con entregables claros.

Criterios a considerar para el cumplimiento de este proceso:

- Traducir los requerimientos del negocio a una especificación de diseño de alto nivel para desarrollo de software, y aprobar las especificaciones de diseño para garantizar que el diseño de alto nivel responde a los requerimientos.
- Preparar el diseño detallado y los requerimientos técnicos del software de aplicación.
- Definir el criterio de aceptación de los requerimientos y aprobar los requerimientos para garantizar que corresponden al diseño de alto nivel.
- Realizar una reevaluación para cuando se presenten discrepancias técnicas o lógicas significativas durante el desarrollo o mantenimiento.
- Asegurar que los controles del negocio se traduzcan correctamente en controles de aplicación de manera que el procesamiento sea exacto, completo, oportuno, aprobado y auditable.
- Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados, de acuerdo con la clasificación de datos, la arquitectura de seguridad en la información de la organización y el perfil de riesgo.
- Personalizar e implantar la funcionalidad automatizada adquirida con el uso de procedimientos de configuración, aceptación y prueba.

- Seguir un proceso de desarrollo similar al de desarrollo de sistemas nuevos en el caso que se presenten modificaciones importantes en los sistemas existentes, que resulten en un cambio significativo de los diseños y/o funcionalidad actuales.
- Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación y los requerimientos de calidad.
- Aprobar y autorizar cada etapa clave del proceso de desarrollo de software aplicativo, dando seguimiento a la terminación exitosa de revisiones de funcionalidad, desempeño y calidad.
- Garantizar que se identifican y consideran todos los aspectos legales y contractuales para el software aplicativo que desarrollan terceros.
- Desarrollar, implantar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización.
- Garantizar que durante el diseño, desarrollo e implantación, se da seguimiento al estatus de los requerimientos particulares (incluyendo todos los requerimientos rechazados), y que las modificaciones a los requerimientos se aprueban a través de un proceso establecido de administración de cambios.
- Desarrollar una estrategia y un plan para el mantenimiento y liberación de aplicaciones de software.

3.2.2.2 AI3: Adquirir y mantener infraestructura tecnológica.

Proporciona las plataformas apropiadas para soportar las aplicaciones del negocio mediante adquisición acertada de hardware, estandarización sobre el software, evaluación del rendimiento del hardware y del software, y administración consistente del sistema.

Criterios a considerar para el cumplimiento de este proceso:

- Genera un plan para adquirir, implantar y mantener a infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización.
- Implanta medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del HW y SW de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.

- Establece ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura en las primeras fases del proceso de adquisición y desarrollo.

3.2.2.3 AI4: Facilitar la operación y el uso

Asegurar el debido uso de las aplicaciones y de las soluciones tecnológicas establecidas, a través de un enfoque estructurado del desarrollo de manuales de procedimiento de usuario y de operaciones, requerimientos de servicio y materiales de entrenamiento.

Criterios a considerar para el cumplimiento de este proceso:

- Desarrolla un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos para llevar acabo las operaciones de TI.
- Transfiere el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos, y ejercer la responsabilidad por la entrega y calidad del servicio, del control interno y de los procesos administrativos de la aplicación.
- Transfiere conocimientos y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de aplicación como apoyo, a los procesos del negocio.
- Transfiere conocimientos y habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos.

3.2.2.4 AI5: Adquirir recursos de TI.

Proveer recursos de TI, incluyendo personas, hardware, software y servicios cuando sea necesario a través de la definición de procesos de abastecimiento, la selección adecuada de proveedores y la configuración de condiciones previamente establecidas.

Criterios a considerar para el cumplimiento de este proceso:

- Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición,

para garantizar que la adquisición de infraestructura, instalaciones, hardware, software y servicios relacionados con TI, satisfagan los requerimientos del negocio.

- Formular un procedimiento para establecer, modificar y concluir contratos que apliquen a todos los proveedores.
- Seleccionar proveedores mediante una práctica justa y formal para garantizar la escogencia del mejor con base en los requerimientos que se han desarrollado con información de proveedores potenciales y acordados entre el cliente y el(los) proveedor(es).
- Incluir y reforzar los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de software involucrados en el suministro y uso continuo de software.
- Incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de recursos de desarrollo.
- Incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales, que comprendan los criterios de aceptación, para la adquisición de infraestructura, instalaciones y servicios relacionados.

3.2.2.5 AI6: Administrar cambios.

Minimizar la probabilidad de interrupción, alteraciones no autorizadas y errores mediante el análisis, la implementación y el seguimiento de todos los cambios solicitados y hechos a la infraestructura existente de TI.

Criterios a considerar para el cumplimiento de este proceso:

- Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.
- Garantizar que todas las solicitudes de cambio se evalúan de una manera estructurada en cuanto a impactos en el sistema operacional y su funcionalidad.
- Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido.
- Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las

aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales.

- Actualizar el sistema asociado y la documentación de usuario y procedimientos siempre que se implantan cambios al sistema.
- Establecer un proceso de revisión para garantizar la implantación completa de los cambios.

3.2.2.6 AI7: Instalar y acreditar soluciones y cambios

Verificar y confirmar que la solución es adecuada para el propósito que se pretende mediante una instalación, migración, conversión y plan de aceptación bien formalizados.

Criterios a considerar para el cumplimiento de este proceso:

- Entrenar al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de desarrollo, implantación o modificación de sistemas de información.
- Establecer un plan de pruebas y obtener la aprobación de las partes relevantes.
- Establecer un plan de implantación y obtener la aprobación de las partes relevantes.
- Establecer un ambiente de prueba que refleje el ambiente futuro de operaciones para permitir pruebas acertadas.
- Garantizar que los componentes sean convertidos del viejo al nuevo sistema de acuerdo con un plan preestablecido.
- Garantizar que se prueban los cambios de acuerdo con el plan de aceptación definido y en base en una evaluación de impacto y recursos.
- Garantizar que los procedimientos proporcionan, como parte de la aceptación final o prueba de aseguramientos de la calidad de los sistemas de información nuevos o modificados, una evaluación formal y la aprobación de los resultados de prueba por parte de la gerencia de los departamentos afectados del usuario y la función de TI.
- Implantar procedimientos formales para controlar la transferencia del sistema desde el ambiente de desarrollo al de pruebas, de acuerdo con el plan de implantación.
- Garantizar que la liberación del software se regula con procedimientos formales que aseguren la autorización, acondicionamiento, pruebas de regresión, distribución,

transferencia de control, rastreo de estatus, procedimientos de respaldo y notificación de usuario.

- Establecer procedimientos de control para asegurar la distribución oportuna y correcta, y la actualización de los componentes aprobados de la configuración.
- Automatizar el sistema utilizado para monitorear cambios a sistemas aplicativos para soportar el registro y rastreo de cambios hechos en aplicaciones, procedimientos, procesos, sistemas y parámetros de servicio, y a las plataformas subyacentes.
- Establecer procedimientos de acuerdo con los estándares de desarrollo y de cambios de la empresa, que requieren una revisión posterior a la implantación del sistema de información en operación para evaluar y reportar si el cambio satisfizo los requerimientos del cliente y entregó los beneficios visualizados, de la forma más rentable.

3.2.3 ENTREGAR Y DAR SOPORTE

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, incluido los aspectos de seguridad y continuidad. Con el fin de proveer servicios, deberán establecer los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

3.2.3.1 DS2: Administrar los servicios de terceros.

Asegurar que los roles y responsabilidades de terceros estén claramente definidos, cumplidos y que continúen satisfaciendo los requerimientos mediante medidas de control dirigidas a la revisión y la monitorización de acuerdos y procedimientos existentes para su efectividad y cumplimiento con la política de la organización.

Criterios a considerar para el cumplimiento de este proceso:

- Identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad.
- Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener una efectiva entrega de servicios de forma segura y eficiente sobre una base de continuidad.

- Asegurar que los contratos están de acuerdo con los estándares universales del negocio de conformidad con los requerimientos legales y regulatorios.
- Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con los requerimientos del negocio actuales y que se apega de manera continua a los acuerdos del contrato y a los convenios de niveles de servicio, y que el desempeño es competitivo respecto a los proveedores alternativos y a las condiciones del mercado.

3.2.3.2 DS3: Administrar el desempeño y la capacidad.

Asegurar que la capacidad adecuada esté disponible y que se haga el mejor y el óptimo uso de ésta, para satisfacer las necesidades requeridas de rendimiento a través de la recolección de datos, análisis y reporte sobre el rendimiento de los recursos, el dimensionamiento de la aplicación y la demanda de carga de trabajo.

Criterios a considerar para el cumplimiento de este proceso:

- Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, con costos justificables, para procesar las cargas de trabajo acordadas tal como se determina en los SLAs.
- Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados.
- Llevar a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño.
- Brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI.
- Monitorear continuamente el desempeño y la capacidad de los recursos de TI.

3.2.3.3 DS4: Garantizar la continuidad del servicio.

Asegurar que los servicios de TI estén disponibles cuando se requieran y asegurar un impacto mínimo en el negocio en el caso de una interrupción importante. Se logra teniendo un plan operativo y probado de continuidad de TI que esté en línea con el plan general de continuidad del negocio y con sus requerimientos de negocio relacionados.

Criterios a considerar para el cumplimiento de este proceso:

- Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización.
- Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio.
- Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.
- Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio.
- Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable.
- Asegurarse de que todos las partes involucradas reciban sesiones de capacitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.
- Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera.
- Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios.
- Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio.

3.2.3.4 DS5: Garantizar la seguridad de los sistemas.

Salvaguardar información contra el uso, revelación o modificación no autorizada, daño o pérdida mediante controles de acceso lógico que aseguran que el acceso a los sistemas, datos y programas esté restringido a los usuarios no autorizados.

Criterios a considerar para el cumplimiento de este proceso:

- Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.
- Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI.
- Identificar de manera única a todos los usuarios y su actividad en sistemas de TI.
- Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario.
- Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.
- Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes.
- Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria.
- Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.
- Garantizar que se cuente con medidas de prevención, detección y corrección a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso.

- Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados para autorizar acceso y controlar los flujos de información desde y hacia las redes.
- Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.

3.2.3.5 DS6: Identificar y asignar costos.

Asegurar un conocimiento correcto de los costos aplicables a los servicios de TI utilizando un sistema de contabilidad de costos que asegura que los costos sean registrados, calculados y asignados al nivel requerido de detalle y a la oferta apropiada de servicio.

Criterios a considerar para el cumplimiento de este proceso:

- Identificar todos los costos de TI y equipararlos a los servicios de TI para soportar un modelo de costos transparente.
- Registrar y asignar los costos actuales de acuerdo con el modelo de costos definido.
- Definir un modelo de costos que incluya costos directos, indirectos y fijos de los servicios, y que ayude al cálculo de tarifas de reintegros de cobro por servicio en base a la definición del servicio.
- Revisar y comparar de forma regular lo apropiado del modelo de costos/recargos para mantener su relevancia para el negocio en evolución y para las actividades de TI.

3.2.3.6 DS7: Educar y entrenar a los usuarios.

Asegurar que los usuarios estén haciendo uso efectivo de la tecnología y que estén concientes de los riesgos y responsabilidades involucradas mediante un extenso plan de entrenamiento y desarrollo.

Criterios a considerar para el cumplimiento de este proceso:

- Establecer y actualizar de forma regular un programa de entrenamiento para cada grupo objetivo de empleados.

3.2.3.7 DS8: Administrar la mesa de servicio y los incidentes.

Asegurar que cualquier problema que experimente el usuario sea resuelto de manera apropiada a través de una facilidad de Help Desk que provee soporte y asesoramiento de primera línea.

Criterios a considerar para el cumplimiento de este proceso:

- Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información.
- Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información.
- Establecer procedimientos de mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente de acuerdo con los límites acordados en el SLA y, si es adecuado, brindar soluciones alternas.
- Garantizar que la asignación de incidentes y el monitoreo del ciclo de vida permanecen en la mesa de servicios, independientemente de qué grupo de TI esté trabajando en las actividades de resolución.
- Establecer procedimientos para el monitoreo puntual de la resolución de consultas de los clientes.
- Emitir reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.

3.2.3.8 DS9: Administrar la configuración.

Dar cuenta de todos los componentes de TI, prevenir las alteraciones no autorizadas, verificar la existencia física y proveer una base para una administración adecuada de cambios. Es posibilitado por controles que identifican y registran todos los activos de TI y su ubicación física, y un programa de verificación regular que confirme su existencia.

Criterios a considerar para el cumplimiento de este proceso:

- Establecer un repositorio central que contenga toda la información referente a los elementos de configuración.

- Revisar y verificar de manera regular, utilizando cuando sea necesario herramientas apropiadas, el estatus de los elementos de configuración para confirmar la integridad de la configuración de datos actual e histórica y para comparar con la situación actual.

3.2.3.9 DS10: Administrar los problemas.

Asegurar que los problemas y los incidentes sean resueltos, y que se investigue la causa para prevenir cualquier recurrencia usando un sistema de administración de problemas que registra y procesa todos los incidentes.

Criterios a considerar para el cumplimiento de este proceso:

- Implementar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes.
- Mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados.
- Identificar e iniciar soluciones sostenibles indicando la causa raíz, incrementando las solicitudes de cambio por medio del proceso de administración de cambios establecido.
- Disponer de un procedimiento para cerrar registros de problemas ya sea después de confirmar la eliminación exitosa del error conocido o después de acordar con el negocio cómo manejar el problema de manera alternativa.
- Garantizar una adecuada administración de problemas e incidentes, integrar los procesos relacionados de administración de cambios, configuración y problemas.

3.2.3.10 DS11: Administrar los datos.

Asegurar que los datos sigan siendo completos, precisos y válidos durante su ingreso, actualización y almacenamiento mediante una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI.

Criterios a considerar para el cumplimiento de este proceso:

- Establecer mecanismos para garantizar que el negocio reciba los documentos originales que espera, que se procese toda la información recibida por parte del negocio, que se preparen y entreguen todos los reportes de salida que requiere el negocio y que las necesidades de reinicio y reproceso estén soportadas.
- Definir e implementar procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables.

- Definir e implementar procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y su uso.
- Definir e implementar procedimientos para prevenir el acceso a datos sensitivos y al software desde equipos o medios una vez que son eliminados o transferidos para otro uso.
- Definir e implementar procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad.
- Establecer mecanismos para identificar y aplicar requerimientos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos.

3.2.3.11 DS12: Administrar el ambiente físico.

Proveer un entorno físico adecuado que proteja el equipo de TI y la gente, contra riesgos naturales y provocados por el hombre. Se logra a través de la instalación de controles ambientales y físicos adecuados que sean revisados regularmente en busca de su funcionamiento apropiado.

Criterios a considerar para el cumplimiento de este proceso:

- Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio.
- Diseñar e implementar medidas de protección contra factores ambientales.

3.2.3.12 DS13: Administrar las operaciones.

Asegurar que las funciones importantes de soporte de TI se realicen regularmente y en la forma debida mediante un programa de actividades de soporte que es registrado y aprobado para la realización de todas las actividades

Criterios a considerar para el cumplimiento de este proceso:

- Definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos.

- Organizar la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el rendimiento y la utilización para cumplir con los requerimientos del negocio.
- Garantizar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones.
- Establecer resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos tales como formas, instrumentos negociables, impresoras de uso especial o dispositivos de seguridad.
- Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.

3.2.4 MONITOREARA Y EVALUAR

Todos los procesos de una organización necesitan ser evaluados regularmente para verificar su calidad y su eficiencia en cuanto a los requerimientos de control, integridad y confidencialidad.

3.2.4.1 ME1: Monitorear y evaluar el desempeño de TI.

Asegurar el logro de los objetivos de rendimiento fijados para los procesos de TI a través de la definición de indicadores relevantes de rendimiento, el reporte sistemático y oportuno del rendimiento y la pronta acción frente a las desviaciones.

Criterios a considerar para el cumplimiento de este proceso:

- Garantizar que la gerencia establezca un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para monitorear la contribución de TI a los resultados de los procesos de administración de programas y de administración del portafolio empresarial y aquellos procesos que son específicos para la entrega de la capacidad y los servicios de TI.
- Garantizar que la gerencia de TI, trabajando en conjunto con el negocio, defina un conjunto balanceado de objetivos, mediciones, metas y comparaciones de desempeño y

que estas se encuentren acordadas formalmente con el negocio y otros interesados relevantes.

- Garantizar que el proceso de monitoreo implante un método, que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa.
- Comparar de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes.
- Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño.
- Identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes.

3.2.4.2 ME2: Monitorear y evaluar el control interno.

Asegurar el logro de los objetivos de control interno fijados para los procesos de TI mediante el compromiso de monitorizar el control interno, determinar su efectividad, y reportar sobre ellos regularmente.

Criterios a considerar para el cumplimiento de este proceso:

- Monitorear de forma continua el ambiente de control y el marco de control de TI.
- Monitorear y reportar la efectividad de los controles internos sobre TI por medio de revisiones de auditoría.
- Registrar la información referente a todas las excepciones de control y garantizar que esto conduzca al análisis de las causas subyacentes y a la toma de acciones correctivas.
- Evaluar la completitud y efectividad de los controles internos de la administración de los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación.
- Obtener, según sea necesario, aseguramiento adicional de la completitud y efectividad de los controles internos por medio de revisiones de terceros.
- Confirmar que los proveedores externos de servicios cumplan con los requerimientos legales y regulatorios y con las obligaciones contractuales.

- Identificar e iniciar medidas correctivas basadas en las evaluaciones y en los reportes de control.

3.2.4.3 ME3: Garantizar el cumplimiento regulatorio.

Cumplir con las obligaciones legales, regulatorias y contractuales identificando y analizando los requerimientos externos para el impacto de TI, y tomando las medidas apropiadas para cumplirlas.

Criterios a considerar para el cumplimiento de este proceso:

- Definir e implantar un proceso para garantizar la identificación oportuna de requerimientos locales e internacionales legales, contractuales, de políticas y regulatorios, relacionados con la información, con la prestación de servicios de información incluyendo servicios de terceros y con la función, procesos e infraestructura de TI.
- Revisar y optimizar las políticas, estándares y procedimientos de TI para garantizar que los requisitos legales y regulatorios se cubran de forma eficiente.
- Evaluar de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requerimientos legales y regulatorios, con base en la supervisión del gobierno de la gerencia de TI y del negocio y la operación de los controles internos.
- Definir e implantar procedimientos para obtener y reportar un aseguramiento del cumplimiento y, donde sea necesario, que el propietario del proceso haya tomado las medidas correctivas oportunas para resolver cualquier brecha de cumplimiento.
- Integrar los reportes de TI sobre cumplimiento regulatorio con las salidas similares provenientes de otras funciones del negocio.

3.2.4.4 ME4: Proporcionar gobierno de TI.

Incluir la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas y de acuerdo con las estrategias y objetivos empresariales.

Criterios a considerar para el cumplimiento de este proceso:

- Trabajar con el consejo directivo para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles y responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI de la empresa ofrezcan y estén alineados con las estrategias y objetivos empresariales.
- Facilitar el entendimiento del consejo directivo y de los ejecutivos sobre temas estratégicos de TI tales como el rol de TI, características propias y capacidades de la tecnología.
- Garantizar que existe un entendimiento compartido entre el negocio y la función de TI sobre la contribución potencial de TI a la estrategia del negocio.
- Trabajar con el consejo directivo para definir e implantar organismos de gobierno, tales como un comité estratégico de TI, para brindar una orientación estratégica a la gerencia respecto a TI.
- Facilitar la alineación de TI con el negocio en lo referente a estrategia y operaciones, fomentando la co-responsabilidad entre el negocio y TI en la toma de decisiones estratégicas y en la obtención de los beneficios provenientes de las inversiones habilitadas con TI.
- Administrar los programas de inversión habilitados con TI, así como otros activos y servicios de TI, para asegurar que ofrezcan el mayor valor posible para apoyar la estrategia y los objetivos empresariales.
- Implantar un enfoque disciplinado hacia la administración por portafolio, programa y proyecto, enfatizando que el negocio asume la propiedad de todas las inversiones habilitadas con TI y que TI garantiza la optimización de los costos por la prestación de los servicios y capacidades de TI.
- Asegurar que las inversiones en tecnología estén estandarizadas a mayor grado posible para evitar el aumento en costo y complejidad de una proliferación de soluciones técnicas.
- Optimizar la inversión, uso y asignación de los activos de TI por medio de evaluaciones periódicas, garantizando que TI cuente con recursos suficientes, competentes y capaces para ejecutar los objetivos estratégicos actuales y futuros y seguir el ritmo de los requerimientos del negocio.
- Trabajar en conjunto con el consejo directivo para definir el nivel de riesgo de TI aceptable por la empresa.

- Comunicar este nivel de riesgo hacia la organización y acordar el plan de administración de riesgos de TI.
- Integrar las responsabilidades de administración de riesgos en la organización, asegurando que tanto el negocio como TI evalúen y reporten periódicamente los riesgos asociados con TI y su impacto en el negocio.
- Garantizar que la gerencia de TI haga seguimiento a la exposición a los riesgos, poniendo especial atención en las fallas y debilidades de control interno y de supervisión, así como su impacto actual y potencial en el negocio.
- Informar el desempeño relevante del portafolio de los programas de TI al consejo directivo y a los ejecutivos de manera oportuna y precisa.
- Garantizar que la organización establezca y mantenga una función competente y que cuente con el personal adecuado y/o busque servicios de aseguramiento externo para proporcionar al consejo directivo.

Para facilitar la aplicación del proceso se ha elaborado un cuestionario (VER ANEXO 4).

3.3 DEFINICIÓN DE ROLES

Antes de la ejecución del proceso se debe tomar en cuenta los roles que están clasificados por procesos.

Algunos procesos específicos tienen un rol adicional especializado, específico para ese proceso.

A continuación se detallan cada uno de los roles:

- Director ejecutivo (CEO)
- Ejecutivos del negocio
- Director de información (CIO)
- Propietario del proceso de negocio
- Jefe de operaciones
- Arquitecto en jefe
- Jefe de desarrollo
- Jefe de administración de TI (para empresas grandes, el jefe de funciones como recursos humanos, presupuestos y control interno)
- Administración de proyectos (PMO)

La siguiente tabla nos muestra los procesos que están ligados a cada uno de los roles.

ROLES	PROCESO
Director ejecutivo (CEO)	PO9, ME4
Ejecutivos del negocio	PO1, ME3
Director de información (CIO)	PO5, PO6, PO8, PO9, PO10, ME4
Propietario del proceso de negocio	DS7
Jefe de operaciones	AI3, AI6, AI7, DS3, DS4, DS5, DS8, DS9, DS10, DS11, DS12, DS13, ME1, ME2
Arquitecto en jefe	PO2, DS5
Jefe de desarrollo	AI2, AI6, AI7, DS8, DS9, DS10, ME1, ME2
Jefe de administración de TI	PO5, PO6, PO7, AI3, AI4, AI5, DS2, DS4, DS6, ME2
Administración de proyectos (PMO)	PO10, AI2, ME3
Departamento de entrenamiento	AI4
Departamento de capacitación	DS7
Gerente de incidentes	DS8
Gerente de configuración	DS9
Gerente de problemas	DS10

Tabla 57: Roles Vs. Procesos

De acuerdo a la realidad de la empresa a la que se vaya aplicar el proceso se debe tomar en cuenta que algunos procesos están ligados a más de un rol, cuando se precisa esto, se debe identificar que el rol esté definido en la empresa, y en el caso de que existan todos los roles el responsable del proceso es el rol de mas alto rango.

3.4 USO DEL PROCESO

Este trabajo ha sido fundamentado en los dominios y subdominios que COBIT 4.0 maneja, se encuentran relacionados con el proceso a través de los aspectos que ésta cubren.

Con el fin de establecer un correcto uso del proceso se empleará la teoría de los valores ponderados de manera que podamos fijar un criterio que ayude a cuantificar los resultados obtenidos de una aplicación.

A continuación detallamos cada uno de los pasos que se debe seguir para el uso correcto del proceso.

3.4.1.1 PASO 1: CARACTERIZACIÓN DE LA EMPRESA

Caracterizar la empresa consiste en conocer y documentar la información tanto de la empresa como de la Unidad Informática, con el fin de establecer los objetivos de la evaluación.

Además ayuda a identificar al personal que ayudaría al evaluador con la documentación legal y de datos de la Unidad Informática de la empresa, ya que muchas veces las empresas no tienen información documentada.

3.4.1.2 PASO 2: APLICACIÓN DEL PROCESO

Previo a la aplicación del proceso se debe tomar en cuenta el proceso específico que le corresponde a cada rol, que se encuentra detallado en la Tabla 57.

3.4.1.3 PASO 3: CUANTIFICACIÓN DE DATOS

Una forma de lograr que el presente trabajo sea fácil de aplicar y que permita enfocar cada punto con su propia importancia es separar cada proceso y cuantificar la totalidad de los puntajes obtenidos para relacionarlos con un porcentaje general que se refiera a cada sección, de manera que sea posible tener una idea acerca de cómo se encuentra determinados los procesos de TI en la empresa.

3.4.1.4 PASO 4: ANÁLISIS DE RESULTADOS

Una vez realizada la cuantificación de datos se debe realizar la interpretación de puntajes obtenidos.

Cada criterio que debe ser respondido tiene asociado un puntaje de la siguiente manera:

RANGO DE PORCENTAJE OBTENIDO	INTERPRETACIÓN
≤ 50 %	Regular
>50% ≤ 75%	Bueno
>75% ≤ 100%	Muy Bueno

Tabla 58: Interpretación de puntajes obtenidos

Se debe tomar en cuenta lo siguiente:

- Si la interpretación es **Regular** se entenderá que es absolutamente necesario tomar medidas inmediatas a fin de evitar problemas y mejorar el aspecto auditado, poniendo gran énfasis en los criterios con bajo puntaje.
- Si la interpretación es **Bueno** se entenderá que es siempre posible mejorar los criterios donde no se ha conseguido un elevado puntaje y que las medidas no son tan inmediatas como el caso anterior. Hay que tomar en cuenta los criterios con alto puntaje de manera que se mantengan en ese estado.
- Si la interpretación es **Muy Bueno** se entenderá que la gestión del aspecto auditado se esta llevando de manera adecuada y que es preciso mantenerlo de esa forma.

3.4.1.5 PASO 5: ANÁLISIS GLOBAL

Al final del análisis de cada proceso se debe concluir el estado actual de la empresa, tomando en cuenta los resultados obtenidos en el paso anterior.

CAPÍTULO 4: APLICACIÓN DEL PROCESO

4.1 JUSTIFICACIÓN DE LA APLICACIÓN EN LA EMPRESA SELECCIONADA.

A continuación se presenta un caso práctico, con el fin de aplicar el proceso propuesto en el capítulo 3, con la ayuda del cuestionario propuesto (VER ANEXO 4) y de acuerdo al análisis del medio que se realizó en el capítulo 2, se ha elegido la empresa privada *GeoInfo*, por la facilidad en la obtención de la información y la acogida que se nos ha brindado.

4.1.1 DESCRIPCIÓN DE LA EMPRESA CASO DE ESTUDIO

GeoInfo es una empresa joven conformada en 1999, con la participación de consultores con una alta experiencia en Soluciones Tecnológicas de información geográfica o Geoinformación que se ha posicionado hoy en día en una de las empresas más importantes si no en la mayor en lo que se refiere al desarrollo de sistemas de georeferenciación.

La solidez profesional de GeoInfo se fundamenta principalmente en la experiencia acumulada, en los convenios y representaciones suscritas con empresas nacionales e internacionales y de su grupo consultor principal, quienes conforman la parte operativa y el soporte complementario de la empresa, los mismos que conjuntamente o individualmente han participado en una gran diversidad de proyectos, lo cual ha acrecentado experiencia y competencia profesional dentro del mercado, traducido a en un liderazgo técnico.

4.1.1.1 Objetivos

- Crear, administrar y desarrollar servicios relacionados con todas las etapas del ciclo de vida de un proyecto o Sistema de Información Geográfica (SIG), y así proveer soluciones integrales a sus Clientes.
- Realizar estudios de factibilidad, definición de procedimientos y otras actividades de consultoría sobre diversas áreas temáticas de SIG, como: Forestal, Minería, Municipalidades, Marketing y Negocios, Medio Ambiente, Mapeo en Internet, Gobierno, Publicación de datos, Cartografía, Transporte, Distribución de Servicios

Básicos (Luz, Agua), Logística y Telecomunicaciones entre las más importantes y otras.

- Brindar diversas alternativas de servicio, para satisfacer totalmente las necesidades de sus clientes. El experimentado equipo profesional está capacitado para evaluar, planificar, coordinar y ejecutar cada uno de los proyectos de servicios.

4.1.2 PLAN DE APLICACIÓN DE LA GUÍA

El presente trabajo consiste en la aplicación del proceso obtenido, a través de la investigación a una empresa que se dedica al desarrollo y comercialización del software geográfico.

En este trabajo están expuestas cada una de las actividades y tareas principales que se realizaron para la aplicación del proceso para la evaluación de TI en la empresa caso estudio; las herramientas utilizadas por el Administrador de TI son encuestas y entrevistas, las mismas que están dirigidas a las personas responsables por parte de la empresa que son el gerente, el administrador de TI. Cabe recalcar que la aplicación del proceso va a ir supervisada por los responsables de la empresa caso de estudio, y que toda la información será manejada bajo un acuerdo de confidencialidad.

Al final de la aplicación del proceso se elaborará un informe que contendrá el resultado del análisis realizado, las conclusiones y las respectivas sugerencias, el informe será verificado por los responsables de la empresa caso de estudio.

4.1.2.1 Diagnóstico de la situación actual de la empresa caso de estudio

4.1.2.1.1 Nombre de la empresa

La empresa se encuentra registrada oficialmente en la superintendencia de Compañías con el nombre de Soluciones Tecnológicas de Geoinformación Cía. Ltda. “GEOINFO”.

4.1.2.1.2 Ubicación Geográfica de GeoInfo

La empresa GeoInfo se encuentra ubicada en Ecuador, dentro del Distrito Metropolitano de Quito, sector centro norte, en las calles Javier Ascazubi y Avenida Diez de Agosto, número E1-16, Edificio Acrusson, Planta baja, oficina número 10.

4.1.2.1.3 Misión

La misión de GeoInfo es trabajar con la meta de desarrollar, difundir y aplicar eficazmente métodos modernos del manejo de la Geoinformática (Tratamiento de la información geográfica con el uso de sistemas informáticos), superando la brecha entre la dinámica de la Tecnología y las necesidades particulares de sus clientes.

4.1.2.1.4 Visión

Mantener el liderazgo de Soluciones Tecnológicas de Geoinformación en el ECUADOR, aplicadas a todas las áreas posibles, en forma directa o mediante alianzas estratégicas.

4.1.2.1.5 Funciones de GeoInfo

Los componentes que conforman la empresa en base a un agrupamiento de actividades similares y propósitos específicos.

GeoInfo, pese a ser una empresa pequeña en relación a su número de integrantes, cuenta con la definición y responsabilidades de cada función que se desarrolla en la empresa, a continuación se describen en forma sucinta cada una de ellas.

Gerencia

Responsable de dictar las directrices que serán seguidas por la empresa, cargo desempeñado por del Ing. Bolívar Viteri, uno de los dos socios de la empresa, experto en diseño, desarrollo e implementación de GIS y de base de datos georeferenciadas, utilizando herramientas GIS estándar de mercado, para múltiples aplicaciones en empresas de Servicios Públicos y Privados como Ambientales, Petroleras, Marketing, Planificación Urbana entre otras.

Presidencia

Responsable de la coordinación del personal de planta y ayudar al Gerente General a que se cumplan con las directrices emanadas por la Gerencia, cargo desempeñado por el otro socio de la empresa, MSc. PHD. Cand. RICHARD RESL, experto en Diseño de Sistemas de Información Geográfica, Manejo de Recursos Naturales, Restitución Digital, Consultor Internacional, Coordinador del Sistema de educación a distancia internacional UNIGIS para América Latina.

Desarrollo de Sistemas

Responsable del Análisis, diseño, desarrollo, implantación y capacitación de los sistemas desarrollados para clientes de GeoInfo, El personal se encuentra a cargo de dos funcionarios que forman parte fija de la empresa, uno responsable de la parte de análisis y diseño, y el otro del desarrollo, implantación y capacitación conjuntamente con un equipo de programadores expertos en el lenguaje que será utilizado para el desarrollo del sistema solicitado, El equipo es contratado temporalmente.

Digitalización

Responsables de realizar las diferentes capas o mapas temáticos que serán utilizados en las consultorías o trabajos solicitados a GeoInfo, el personal es de reconocida experiencia en la rama, generalmente está conformado por geógrafos y se le contrata para trabajos específicos y se apoya igualmente de un grupo de pasantes, no son personal de planta, solo de apoyo.

Campo

Responsables de realizar levantamiento de datos requeridos en el campo, como catastros, encuestas, ubicaciones, etc., de igual forma el personal es contratado temporalmente acorde a las necesidades de los trabajos solicitados y cuenta con la experiencia suficiente para realizar los trabajos encomendados.

4.1.3 APLICACIÓN DEL PROCESO

PLANIFICAR Y ORGANIZAR

PO1: Definir un plan estratégico para TI

FACTORES A CONSIDERAR PARA DEFINIR UN PLAN ESTRATÉGICO DE TI **Se debe verificar si:**	SI	PARCIALMENTE	NO
Tiene definido un plan estratégico de TI y este se encuentra alineado con las necesidades del negocio.	✓		
Realiza la evaluación del desempeño de los planes existentes y de los sistemas de información.	✓		
Traduce el plan estratégico de TI a planes tácticos.		✓	
Analiza portafolios de programas y se administra portafolios de servicios y proyectos.			✓

PO2: Definir la arquitectura de la información

FACTORES A CONSIDERAR PARA DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN **Se debe verificar si:**	SI	PARCIALMENTE	NO
Tiene definida la arquitectura de la información.		✓	
Cuenta con un diccionario de datos empresarial.			✓

PO5: Administrar la inversión en TI.

FACTORES A CONSIDERAR PARA ADMINISTRAR LA INVERSIÓN EN TI. **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece un marco de trabajo financiero para TI que impulse el presupuesto y el análisis de rentabilidad, con base en los portafolios de inversión, servicios y activos.	✓		
Se implanta un proceso de toma de decisiones para dar prioridades a la asignación de recursos de TI.		✓	
Establece y mantiene un proceso presupuestal de TI.		✓	
Implanta un proceso de administración de costos que compare los costos reales con los presupuestados.		✓	
Implanta un proceso de monitoreo de beneficios		✓	

PO6: Comunicar las aspiraciones y la dirección de la gerencia.

FACTORES A CONSIDERAR PARA COMUNICAR LAS ASPIRACIONES Y LA DIRECCIÓN DE LA GERENCIA **Se debe verificar si:**	SI	PARCIALMENTE	NO
Define los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa.		✓	
Elabora y da mantenimiento a un marco de trabajo enfocado en los riesgos y control interno, para entregar valor mientras al mismo tiempo se protegen los recursos y sistemas de TI.			✓
Elabora y da mantenimiento a un conjunto de políticas que apoyen la estrategia de TI.	✓		
Implantan y comunican las políticas de TI al personal que le compete.		✓	
Asegura que la conciencia y el entendimiento de los objetivos de la			✓

dirección del negocio y de TI se comunican a toda la organización.			

PO7: Administrar los recursos humanos de TI

FACTORES A CONSIDERAR PARA ADMINISTRAR LOS RECURSOS HUMANOS DE TI **Se debe verificar si:**	SI	PARCIALMENTE	NO
Asegura que el reclutamiento del personal de TI se lleve a cabo de acuerdo a políticas y procedimientos generales de personal de la organización.	✓		
Verifica periódicamente que el personal este capacitado.	✓		
Define, monitorea y supervisa los marcos de trabajo para los roles, responsabilidades y compensación del personal en base a políticas administrativas.		✓	
Capacita constantemente al personal de TI.	✓		
Minimiza el grado de dependencia del personal indispensable.		✓	
Minimiza el riesgo del cambio de puesto o terminación del trabajo del personal.	✓		

PO8: Administrar la calidad

FACTORES A CONSIDERAR PARA ADMINISTRAR LA CALIDAD **Se debe verificar si:**	SI	PARCIALMENTE	NO
Monitorea y mide la efectividad y aceptación del QMS y lo mejora cuando sea necesario.	✓		
Identifica y mantiene estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del QMS.		✓	
Adopta y mantiene estándares para todo el desarrollo y adquisición que sigue el ciclo de vida hasta el último entregable.		✓	
Garantiza que la administración de calidad se enfoquen los clientes, determine sus requerimientos y los alinee con los estándares y prácticas de TI.		✓	
Elabora y comunica un plan global de calidad que promueva la mejora continua, de forma periódica.	✓		
Define, planea e implementa mediciones para monitorear el		✓	

cumplimiento continuo del QMS, así como el valor que este proporciona.			

PO9: Evaluar y administrar los riesgos de TI.

FACTORES A CONSIDERAR PARA EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI. **Se debe verificar si:**	SI	PARCIALMENTE	NO
Integra el gobierno, la administración de riesgos y el marco de control de TI., al marco de trabajo de administración de riesgos de la organización.	✓		
Establece el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados.	✓		
Identifica las amenazas y vulnerabilidades que afectan al normal desempeño de la empresa.		✓	
Evalúa de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos.	✓		
Elabora y mantiene respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continua.		✓	
Asigna prioridades y planea las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarios, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución.		✓	

PO10: Administrar Proyectos

FACTORES A CONSIDERAR PARA ADMINISTRAR PROYECTOS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Mantiene el programa de los proyectos, relacionados con el portafolio de los programas de inversión en TI.		✓	
Establece y mantiene un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas.			✓
Establece un enfoque de administración de proyectos que		✓	

corresponda al tamaño complejidad y requerimientos regulatorios de cada proyecto.			
Asegura que todos los proyectos de TI cuenten con patrocinadores con la suficiente autoridad para apropiarse de la ejecución del proyecto dentro del programa estratégico global.		✓	
Obtiene el compromiso y participación de los interesados afectados en la definición y ejecución del proyecto dentro del contexto del programa global de inversión en TI.		✓	
Define y documenta la naturaleza y alcance del proyecto para conformar y desarrollar, entre los interesados, un entendimiento común del alcance del proyecto y su relación con otros proyectos dentro del programa global de inversiones en TI.	✓		
Asegura que el arranque de las etapas importantes del proyecto se aprueben de manera formal y se comunique a todos los interesados.		✓	
Establece un plan integrado para el proyecto, aprobado y formal para guiar la ejecución y control del proyecto a lo largo de la vida de este.		✓	
Entiende y documenta dentro de un mismo programa las actividades e interdependencias de múltiples proyectos.	✓		
Define las responsabilidades, relaciones, autoridades y criterios de desempeño de los miembros del equipo del proyecto y especifica las bases para adquirir y asignar a los miembros competentes del equipo y/o los contratistas al proyecto.		✓	
Eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, análisis, respuesta, monitoreo y control de las áreas o eventos que tenga el potencial de ocasionar cambios no deseados.		✓	
Prepara un plan de administración de la calidad que describa el sistema de calidad del proyecto y como será implantado.	✓		
Revisa y acuerda el plan de calidad de proyecto con todas las partes interesadas para luego ser incorporado en el plan integrado del proyecto.	✓		
Establece un sistema de control de cambios para cada proyecto, de tal modo que todos los cambios a la línea base del proyecto se			✓

revisen, aprueben e incorporen de manera apropiada al plan integrado del proyecto, de acuerdo al marco de trabajo del gobierno del programa y del proyecto.			
Identifica las tareas de aseguramiento requeridas para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado.			✓
Mide el desempeño del proyecto contra los criterios claves del proyecto y recomienda, implanta y monitorea las medidas correctivas según sea requerido, de acuerdo con el marco de trabajo de gobierno del programa y del proyecto.		✓	
Solicita que al finalizar cada proyecto, los interesados del proyecto se cercioren de que el proyecto haya cubierto los resultados y beneficios esperados.		✓	

ADQUIRIR E IMPLEMENTAR

AI2: Adquirir y mantener software aplicativo.

FACTORES A CONSIDERAR PARA ADQUIRIR Y MANTENER SOFTWARE APLICATIVO. **Se debe verificar si:**	SI	PARCIALMENTE	NO
Traduce los requerimientos del negocio a una especificación de diseño de alto nivel para desarrollo de software, y aprueba las especificaciones de diseño para garantizar que el diseño de alto nivel responde a los requerimientos.	✓		
Prepara el diseño detallado y los requerimientos técnicos del software de aplicación.	✓		
Define el criterio de aceptación de los requerimientos y aprobar los requerimientos para garantizar que corresponden al diseño de alto nivel.		✓	
Realiza una reevaluación para cuando se presenten discrepancias técnicas o lógicas significativas durante el desarrollo o mantenimiento.	✓		
Asegura que los controles del negocio se traduzcan correctamente en controles de aplicación de manera que el procesamiento sea exacto, completo, oportuno, aprobado y auditable.	✓		
Aborda la seguridad de las aplicaciones y los requerimientos de	✓		

disponibilidad en respuesta a los riesgos identificados, de acuerdo con la clasificación de datos, la arquitectura de seguridad en la información de la organización y el perfil de riesgo.			
Personaliza e implanta la funcionalidad automatizada adquirida con el uso de procedimientos de configuración, aceptación y prueba.		✓	
Sigue un proceso de desarrollo similar al de desarrollo de sistemas nuevos en el caso que se presenten modificaciones importantes en los sistemas existentes, que resulten en un cambio significativo de los diseños y/o funcionalidad actuales.		✓	
Garantiza que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación y los requerimientos de calidad.		✓	
Aprueba y autoriza cada etapa clave del proceso de desarrollo de software aplicativo, dando seguimiento a la terminación exitosa de revisiones de funcionalidad, desempeño y calidad.		✓	
Garantiza que se identifican y consideran todos los aspectos legales y contractuales para el software aplicativo que desarrollan terceros.	✓		
Desarrolla, implanta los recursos y ejecuta un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización.		✓	
Garantiza que durante el diseño, desarrollo e implantación, se da seguimiento al estatus de los requerimientos particulares (incluyendo todos los requerimientos rechazados), y que las modificaciones a los requerimientos se aprueban a través de un proceso establecido de administración de cambios.		✓	
Desarrolla una estrategia y un plan para el mantenimiento y liberación de aplicaciones de software.		✓	

AI3: Adquirir y mantener infraestructura tecnológica.

FACTORES A CONSIDERAR PARA ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA. Se debe verificar si:	SI	PARCIALMENTE	NO

Genera un plan para adquirir, implantar y mantener a infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización.	✓		
Implanta medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del HW y SW de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.		✓	
Establece ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura en las primeras fases del proceso de adquisición y desarrollo.	✓		

AI4: Facilitar la operación y el uso

FACTORES A CONSIDERAR PARA FACILITAR LA OPEERACIÓN Y EL USO **Se debe verificar si:**	SI	PARCIALMENTE	NO
Desarrolla un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos para llevar acabo las operaciones de TI.		✓	
Transfiere el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos, y ejercer la responsabilidad por la entrega y calidad del servicio, del control interno y de los procesos administrativos de la aplicación.		✓	
Transfiere conocimientos y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de aplicación como apoyo, a los procesos del negocio.	✓		
Transfiere conocimientos y habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos.		✓	

AI5: Adquirir recursos de TI.

FACTORES A CONSIDERAR PARA ADQUIRIR	SI	PARCIALMENTE	NO

RECURSOS DE TI **Se debe verificar si:**			
Desarrolla y sigue un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición, para garantizar que la adquisición de infraestructura, instalaciones, hardware, software y servicios relacionados con TI, satisfagan los requerimientos del negocio.	✓		
Formula un procedimiento para establecer, modificar y concluir contratos que apliquen a todos los proveedores.	✓		
Selecciona proveedores mediante una práctica justa y formal para garantizar la escogencia del mejor con base en los requerimientos que se han desarrollado con información de proveedores potenciales y acordados entre el cliente y el(los) proveedor(es).	✓		
Incluye y refuerza los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de software involucrados en el suministro y uso continuo de software.	✓		
Incluye y hace cumplir los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de recursos de desarrollo.	✓		
Incluye y hace cumplir los derechos y obligaciones de todas las partes en los términos contractuales, que comprendan los criterios de aceptación, para la adquisición de infraestructura, instalaciones y servicios relacionados.	✓		

AI6: Administrar cambios

FACTORES A CONSIDERAR PARA ADMINISTRAR CAMBIOS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.			✓
Garantiza que todas las solicitudes de cambio se evalúan de una manera estructurada en cuanto a impactos en el sistema		✓	

operacional y su funcionalidad.			
Establece un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido.		✓	
Establece un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales.	✓		
Actualiza el sistema asociado y la documentación de usuario y procedimientos siempre que se implantan cambios al sistema.		✓	
Establece un proceso de revisión para garantizar la implantación completa de los cambios.		✓	

AI7: Instalar y acreditar soluciones y cambios.

FACTORES A CONSIDERAR PARA INSTALAR Y ACREDITAR SOLUCIONES Y CAMBIOS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Entrena al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de desarrollo, implantación o modificación de sistemas de información.		✓	
Establece un plan de pruebas y obtener la aprobación de las partes relevantes.	✓		
Establece un plan de implantación y obtener la aprobación de las partes relevantes.	✓		
Establece un ambiente de prueba que refleje el ambiente futuro de operaciones para permitir pruebas acertadas.		✓	
Garantiza que los componentes sean convertidos del viejo al nuevo sistema de acuerdo con un plan preestablecido.		✓	
Garantiza que se prueban los cambios de acuerdo con el plan de aceptación definido y en base en una evaluación de impacto y recursos.			✓
Garantiza que los procedimientos proporcionan, como parte de la		✓	

aceptación final o prueba de aseguramientos de la calidad de los sistemas de información nuevos o modificados, una evaluación formal y la aprobación de los resultados de prueba por parte de la gerencia de los departamentos afectados del usuario y la función de TI.			
Implanta procedimientos formales para controlar la transferencia del sistema desde el ambiente de desarrollo al de pruebas, de acuerdo con el plan de implantación.		✓	
Garantiza que la liberación del software se regula con procedimientos formales que aseguren la autorización, acondicionamiento, pruebas de regresión, distribución, transferencia de control, rastreo de estatus, procedimientos de respaldo y notificación de usuario.	✓		
Establece procedimientos de control para asegurar la distribución oportuna y correcta, y la actualización de los componentes aprobados de la configuración.		✓	
Automatiza el sistema utilizado para monitorear cambios a sistemas aplicativos para soportar el registro y rastreo de cambios hechos en aplicaciones, procedimientos, procesos, sistemas y parámetros de servicio, y a las plataformas subyacentes.	✓		
Establece procedimientos de acuerdo con los estándares de desarrollo y de cambios de la empresa, que requieren una revisión posterior a la implantación del sistema de información en operación para evaluar y reportar si el cambio satisfizo los requerimientos del cliente y entregó los beneficios visualizados, de la forma más rentable.		✓	

ENTREGAR Y DAR SOPORTE

DS2: Administrar servicios de terceros.

FACTORES A CONSIDERAR PARA ADMINISTRAR SERVICIOS DE TERCEROS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad.			✓
Identificar y mitigar los riesgos relacionados con la habilidad de			✓

los proveedores para mantener una efectiva entrega de servicios de forma segura y eficiente sobre una base de continuidad.			
Asegurar que los contratos están de acuerdo con los estándares universales del negocio de conformidad con los requerimientos legales y regulatorios.		✓	
Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con los requerimientos del negocio actuales y que se apega de manera continua a los acuerdos del contrato y a los convenios de niveles de servicio, y que el desempeño es competitivo respecto a los proveedores alternativos y a las condiciones del mercado.		✓	

DS3: Administrar desempeño y capacidad.

FACTORES A CONSIDERAR PARA EVALUAR Y FACTORES A CONSIDERAR PARA ADMINISTRAR DESEMPEÑO Y CAPACIDAD **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, con costos justificables, para procesar las cargas de trabajo acordadas tal como se determina en los SLAs.		✓	
Revisa la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados.		✓	
Lleva a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño.	✓		
Brinda la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI.		✓	
Monitorea continuamente el desempeño y la capacidad de los		✓	

recursos de TI.			

DS4: Garantizar la continuidad del servicio.

FACTORES A CONSIDERAR PARA GARANTIZAR LA CONTINUIDAD DEL SERVICIO. **Se debe verificar si:**	SI	PARCIALMENTE	NO
Desarrolla un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización.	✓		
Desarrolla planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio.		✓	
Centra la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.	✓		
Exhorta a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio.	✓		
Prueba el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable.		✓	
Asegura de que todos las partes involucradas reciban sesiones de capacitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.		✓	
Determina que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera.		✓	
Planea las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios.	✓		
Almacena fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio.		✓	

DS5: Garantizar la seguridad de los sistemas

FACTORES A CONSIDERAR PARA GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Administra la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.		✓	
Traslada los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI.	✓		
Identifica de manera única a todos los usuarios y su actividad en sistemas de TI.	✓		
Garantiza que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario.	✓		
Garantiza que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.		✓	
Garantiza que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes.		✓	
Garantiza que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria.	✓		
Determina que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.		✓	
Garantiza que se cuente con medidas de prevención, detección y corrección a lo largo de toda la organización para proteger a los		✓	

sistemas de información y a la tecnología contra software malicioso			
Garantiza que se utilizan técnicas de seguridad y procedimientos de administración asociados para autorizar acceso y controlar los flujos de información desde y hacia las redes.		✓	
Garantiza que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.		✓	

DS6: Identificar y asignar costos

FACTORES A CONSIDERAR PARA IDENTIFICAR Y ASIGNAR COSTOS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Identifica todos los costos de TI y equipararlos a los servicios de TI para soportar un modelo de costos transparente.	✓		
Registra y asigna los costos actuales de acuerdo con el modelo de costos definido.	✓		
Define un modelo de costos que incluya costos directos, indirectos y fijos de los servicios, y que ayude al cálculo de tarifas de reintegros de cobro por servicio en base a la definición del servicio.		✓	
Revisa y compara de forma regular lo apropiado del modelo de costos/recargos para mantener su relevancia para el negocio en evolución y para las actividades de TI.	✓		

DS7: Educar y entrenar a los usuarios

FACTORES A CONSIDERAR PARA EDUCAR Y ENTRENAR A LOS USUARIOS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece y actualiza de forma regular un programa de entrenamiento para cada grupo objetivo de empleados,	✓		

DS8: Administrar la mesa de servicio y los incidentes

FACTORES A CONSIDERAR PARA ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información.		✓	
Establece una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información.	✓		
Establece procedimientos de mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente de acuerdo con los límites acordados en el SLA y, si es adecuado, brindar soluciones alternas.		✓	
Garantiza que la asignación de incidentes y el monitoreo del ciclo de vida permanecen en la mesa de servicios, independientemente de qué grupo de TI esté trabajando en las actividades de resolución.			✓
Establece procedimientos para el monitoreo puntual de la resolución de consultas de los clientes.		✓	
Emite reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.		✓	

DS9: Administrar la configuración

FACTORES A CONSIDERAR PARA ADMINISTRACIÓN DE LA CONFIGURACIÓN **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece un repositorio central que contenga toda la información referente a los elementos de configuración.	✓		
Revisa y verifica de manera regular, utilizando cuando sea necesario herramientas apropiadas, el estatus de los elementos de		✓	

configuración para confirmar la integridad de la configuración de datos actual e histórica y para comparar con la situación actual.			

DS10: Administración de problemas

FACTORES A CONSIDERAR PARA ADMINISTRACIÓN DE PROBLEMAS **Se debe verificar si**	SI	PARCIALMENTE	NO
Implementa procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes		✓	
Mantiene pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados.		✓	
Identifica e inicia soluciones sostenibles indicando la causa raíz, incrementando las solicitudes de cambio por medio del proceso de administración de cambios establecido.	✓		
Dispone de un procedimiento para cerrar registros de problemas ya sea después de confirmar la eliminación exitosa del error conocido o después de acordar con el negocio cómo manejar el problema de manera alternativa.	✓		
Garantiza una adecuada administración de problemas e incidentes, integrar los procesos relacionados de administración de cambios, configuración y problemas.		✓	

DS11: Administración de la Información

FACTORES A CONSIDERAR PARA ADMINISTRACIÓN DE LA INFORMACIÓN **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece mecanismos para garantizar que el negocio reciba los documentos originales que espera, que se procese toda la información recibida por parte del negocio, que se preparen y entreguen todos los reportes de salida que requiere el negocio y que las necesidades de reinicio y reproceso estén soportadas.	✓		
Define e implementa procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables.		✓	

Define e implementa procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y su uso.		✓	
Define e implementa procedimientos para prevenir el acceso a datos sensitivos y al software desde equipos o medios una vez que son eliminados o transferidos para otro uso.		✓	
Define e implementa procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad.		✓	
Establece mecanismos para identificar y aplicar requerimientos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos.		✓	

DS12: Administración del ambiente físico.

FACTORES A CONSIDERAR PARA ADMINISTRACIÓN DEL AMBIENTE FÍSICO **Se debe verificar si::**	SI	PARCIALMENTE	NO
Define e implementa medidas de seguridad físicas alineadas con los requerimientos del negocio.	✓		
Diseña e implementa medidas de protección contra factores ambientales.		✓	

DS13: Administración de Operaciones

FACTORES A CONSIDERAR PARA ADMINISTRACIÓN DE OPERACIONES **Se debe verificar si:**	SI	PARCIALMENTE	NO
Define, implementa y mantiene procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos.	✓		
Organiza la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el rendimiento y la utilización para cumplir con los requerimientos del negocio.		✓	
Garantiza que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las	✓		

otras actividades que soportan o que están alrededor de las operaciones.			
Establece resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos tales como formas, instrumentos negociables, impresoras de uso especial o dispositivos de seguridad.	✓		
Define e implementa procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.	✓		

MONITOREAR Y EVALUAR

ME1: Monitorear y evaluar el desempeño de TI.

FACTORES A CONSIDERAR PARA MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI **Se debe verificar si::**	SI	PARCIALMENTE	NO
Garantiza que la gerencia establezca un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para monitorear la contribución de TI a los resultados de los procesos de administración de programas y de administración del portafolio empresarial y aquellos procesos que son específicos para la entrega de la capacidad y los servicios de TI.		✓	
Garantiza que la gerencia de TI, trabajando en conjunto con el negocio, defina un conjunto balanceado de objetivos, mediciones, metas y comparaciones de desempeño y que estas se encuentren acordadas formalmente con el negocio y otros interesados relevantes.		✓	
Garantiza que el proceso de monitoreo implante un método, que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa.	✓		
Compara de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes.		✓	
Proporciona reportes administrativos para ser revisados por la alta		✓	

dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño.			
Identifica e inicia medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes.		✓	

ME2: Monitorear y evaluar el control interno.

FACTORES A CONSIDERAR PARA FACTORES A CONSIDERAR PARA MONITOREAR Y EVALUAR EL CONTROL INTERNO **Se debe verificar:**	SI	PARCIALMENTE	NO
Monitorea de forma continua el ambiente de control y el marco de control de TI.		✓	
Monitorea y reporta la efectividad de los controles internos sobre TI por medio de revisiones de auditoría.		✓	
Registra la información referente a todas las excepciones de control y garantizar que esto conduzca al análisis de las causas subyacentes y a la toma de acciones correctivas.		✓	
Evalúa la completitud y efectividad de los controles internos de la administración de los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación.	✓		
Obtiene, según sea necesario, aseguramiento adicional de la completitud y efectividad de los controles internos por medio de revisiones de terceros.		✓	
Confirma que los proveedores externos de servicios cumplan con los requerimientos legales y regulatorios y con las obligaciones contractuales.		✓	
Identifica e inicia medidas correctivas basadas en las evaluaciones y en los reportes de control.	✓		

ME3: Garantizar el cumplimiento regulatorio.

FACTORES A CONSIDERAR PARA GARANTIZAR EL CUMPLIMIENTO REGULATORIO.	SI	PARCIALMENTE	NO

Se debe verificar si:			
Define e implanta un proceso para garantizar la identificación oportuna de requerimientos locales e internacionales legales, contractuales, de políticas y regulatorios, relacionados con la información, con la prestación de servicios de información incluyendo servicios de terceros y con la función, procesos e infraestructura de TI.		✓	
Revisa y optimiza las políticas, estándares y procedimientos de TI para garantizar que los requisitos legales y regulatorios se cubran de forma eficiente.			✓
Evalúa de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requerimientos legales y regulatorios, con base en la supervisión del gobierno de la gerencia de TI y del negocio y la operación de los controles internos.		✓	
Define e implanta procedimientos para obtener y reportar un aseguramiento del cumplimiento y, donde sea necesario, que el propietario del proceso haya tomado las medidas correctivas oportunas para resolver cualquier brecha de cumplimiento.		✓	
Integra los reportes de TI sobre cumplimiento regulatorio con las salidas similares provenientes de otras funciones del negocio.		✓	

ME4: Proporcionar Gobierno de TI.

FACTORES A CONSIDERAR PARA PROPORCIONAR GOBIERNO DE TI. **Se debe verificar si:**	SI	PARCIALMENTE	NO
Trabaja con el consejo directivo para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles y responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI de la empresa ofrezcan y estén alineados con las estrategias y objetivos empresariales.			✓
Facilita el entendimiento del consejo directivo y de los ejecutivos sobre temas estratégicos de TI tales como el rol de TI, características propias y capacidades de la tecnología.		✓	

Garantiza que existe un entendimiento compartido entre el negocio y la función de TI sobre la contribución potencial de TI a la estrategia del negocio.		✓	
Trabaja con el consejo directivo para definir e implantar organismos de gobierno, tales como un comité estratégico de TI, para brindar una orientación estratégica a la gerencia respecto a TI.		✓	
Facilita la alineación de TI con el negocio en lo referente a estrategia y operaciones, fomentando la co-responsabilidad entre el negocio y TI en la toma de decisiones estratégicas y en la obtención de los beneficios provenientes de las inversiones habilitadas con TI.		✓	
Administra los programas de inversión habilitados con TI, así como otros activos y servicios de TI, para asegurar que ofrezcan el mayor valor posible para apoyar la estrategia y los objetivos empresariales.			✓
Implanta un enfoque disciplinado hacia la administración por portafolio, programa y proyecto, enfatizando que el negocio asume la propiedad de todas las inversiones habilitadas con TI y que TI garantiza la optimización de los costos por la prestación de los servicios y capacidades de TI.		✓	
Asegura que las inversiones en tecnología estén estandarizadas a mayor grado posible para evitar el aumento en costo y complejidad de una proliferación de soluciones técnicas.		✓	
Optimiza la inversión, uso y asignación de los activos de TI por medio de evaluaciones periódicas, garantizando que TI cuente con recursos suficientes, competentes y capaces para ejecutar los objetivos estratégicos actuales y futuros y seguir el ritmo de los requerimientos del negocio.		✓	
Trabaja en conjunto con el consejo directivo para definir el nivel de riesgo de TI aceptable por la empresa.	✓		
Comunica este nivel de riesgo hacia la organización y acordar el plan de administración de riesgos de TI.		✓	
Integra las responsabilidades de administración de riesgos en la organización, asegurando que tanto el negocio como TI evalúen y reporten periódicamente los riesgos asociados con TI y su impacto		✓	

en el negocio.			
Garantiza que la gerencia de TI haga seguimiento a la exposición a los riesgos, poniendo especial atención en las fallas y debilidades de control interno y de supervisión, así como su impacto actual y potencial en el negocio.	✓		
Informa el desempeño relevante del portafolio de los programas de TI al consejo directivo y a los ejecutivos de manera oportuna y precisa.		✓	
Garantiza que la organización establezca y mantenga una función competente y que cuente con el personal adecuado y/o busque servicios de aseguramiento externo para proporcionar al consejo directivo.			✓

Los resultados de la aplicación del proceso se encuentran definidos en el ANEXO 5.

4.2ANÁLISIS DE LOS RESULTADOS OBTENIDOS

4.2.1 ANÁLISIS POR PROCESOS

PLANIFICAR Y ORGANIZAR

PO1: Definir un plan estratégico para TI

La empresa tiene implantado el plan estratégico de TI, sin embargo no es adecuada la administración de portafolios de TI.

Es necesario considerar que dicho plan debe estar debidamente actualizado, tomando en cuenta el análisis de portafolios de programas y la administración de portafolios de servicios y proyectos, siendo estas las falencias que se han encontrado en la empresa.

PO2: Definir la arquitectura de la información

La organización tiene definida la arquitectura de la información, pero no facilita la creación, uso y compartición óptimas de la información por parte del negocio. Los sistemas existentes no son los apropiados para optimizar el uso de esta información.

No cuenta con un diccionario de datos empresarial, lo que indica que al momento de la toma de decisiones gerenciales no son las más adecuadas, impidiendo asegurar que se proporciona información confiable y segura.

Es necesario mantener un repositorio automatizado de datos y diccionario de datos y que existan reglas de sintaxis de datos.

PO5: Administrar la inversión en TI.

Se debe administrar las inversiones de TI, las mismas que deben ser comunicadas de manera formal al gerente general, de esta manera todos los gastos que se tengan en la empresa siempre sean justificados para que existan respaldos que documenten aquellas inversiones, logrando así un financiamiento y control del desembolso de los recursos financieros de manera segura y apropiada.

Actualmente se esta cumpliendo con los requisitos pero es importante tomar en cuenta que se puede mejorar el marco de trabajo para administrar los programas de inversión en TI.

PO6: Comunicar las aspiraciones y la dirección de la gerencia.

Se tiene implantado un marco de trabajo de control empresarial para TI, sin embargo mediante la aplicación del proceso se ha determinado que no se cumple satisfactoriamente.

Para lo cual se debe definir, elaborar y dar mantenimiento a un marco de trabajo enfocado en los riesgos y control interno.

Además se debe asegurar que la conciencia y el entendimiento de los objetivos de la dirección del negocio y de TI se comunican a toda la organización.

PO7: Administrar los recursos humanos de TI

La administración del recurso humano de TI se encuentra en un nivel aceptable, ya que la empresa cuenta con poco personal lo cual facilita la administración del mismo.

PO8: Administrar la calidad

En los resultados del análisis se puede ver claramente que la administración de la calidad se cumple en gran parte, sin embargo presenta algunas falencias que deben ser tomadas en cuenta para una correcta administración.

Se debe identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI, y para todo el desarrollo y adquisición que sigue el ciclo de vida hasta el último entregable y garantizar que la administración de calidad se enfoque en los clientes.

PO9: Evaluar y administrar los riesgos de TI.

Podemos decir que se tiene una adecuada administración de los riesgos de TI, aunque se puede ver que existen ciertos problemas.

Se debe llevar un plan de acción de riesgos que permita realizar el análisis, evaluación y mitigación de los mismos, logrando con ello que la empresa pueda responder a las amenazas que se pueden presentar.

PO10: Administrar Proyectos

En la empresa tiene establecido métodos para la administración de proyectos de TI, sin embargo es necesario considerar que se debe establecer un enfoque de administración de proyectos que corresponda al tamaño, complejidad y requerimientos regulatorios de cada proyecto, e identificar las tareas de aseguramiento requeridas para apoyar la acreditación de sistemas nuevos o modificados.

Se debe medir el desempeño de los proyectos contra los criterios claves de los proyectos, una vez medido, recomendar, implantar y monitorear las medidas correctivas, de acuerdo con el marco de trabajo de gobierno del programa y del proyecto.

Resumen del dominio Planear y Organizar

En base al análisis por procesos realizado se puede determinar que el dominio Planear y Organizar se esta llevando a cabo, pero es posible mejorar los criterios que no se están cumpliendo a cabalidad.

Los objetivos del negocio están siendo cubiertos por las TI, mediante las estrategias y las tácticas definidas en la empresa. Para que la visión estratégica se cumpla en su totalidad necesita ser planeada, comunicada y administrada desde diferentes perspectivas y finalmente se deberá establecer una organización y una infraestructura tecnológica apropiadas.

ADQUIRIR E IMPLEMENTAR

AI2: Adquirir y mantener software aplicativo.

Se constato que la operatividad del negocio se desarrolla de forma apropiada con las aplicaciones automatizadas respectivas. Empero se recomienda:

Que se realicen pruebas funcionales y de aceptación continuamente en cada proyecto que se vaya a ejecutar. Y que se lleve un control del ciclo de vida de software de aplicación usado en la empresa.
Es conveniente desarrollar una estrategia y un plan para el mantenimiento y liberación de aplicaciones de software.

AI3: Adquirir y mantener infraestructura tecnológica.
Los procesos para adquirir, implantar y actualizar la infraestructura tecnológica son los adecuados lo que garantiza que existe un soporte tecnológico continuo para las aplicaciones del negocio.

AI4: Facilitar la operación y el uso
En los resultados del análisis realizado se puede determinar que el conocimiento sobre los nuevos sistemas no esta del todo disponible.
Se recomienda la generación de documentación y manuales para usuarios y para TI, así como también proporcionar entrenamiento para garantizar el uso y la operación correcta de las aplicaciones y de la infraestructura.

AI5: Adquirir recursos de TI.
La adquisición de recursos de TI es la apropiada y es preciso mantenerlo de esa forma.

AI6: Administrar cambios
La empresa no lleva un proceso formal para la administración de cambios, es decir simplemente lleva un control de cambios establecidos por ellos mismos en hojas de cálculo o papel. Se recomienda que la empresa cuente con una correcta identificación de cambios, en donde deben existir procedimientos de categorización, priorización y emergencia de cambios para una correcta evaluación del impacto de los mismos.

AI7: Instalar y acreditar soluciones y cambios.
Se constato que la empresa avala de alguna manera que los sistemas operacionales estén en línea con las expectativas convenidas y con los resultados esperados. Sin embargo debe tomar en cuenta que los cambios de acuerdo con el plan de aceptación definido y en base a la evaluación de impacto y de los recursos, garanticen que los sistemas nuevos o

modificados con los que cuenta, trabajen sin problemas significativos después de la instalación.

Resumen del dominio Adquirir e Implementar

Según los resultados obtenidos podemos concluir que este dominio se esta cumpliendo casi en su totalidad, no obstante se debe poner más énfasis en alguno de sus procesos.

Las soluciones de TI están siendo identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio, los nuevos proyectos que están desarrollándose son entregados a tiempo y dentro del presupuesto acordado, los mismos que trabajan apropiadamente al momento de su implantación.

Además se debe cubrir los cambios y el mantenimiento realizados a los sistemas existentes sin alterar las actuales operaciones de la empresa.

ENTREGAR Y DAR SOPORTE

DS2: Administrar servicios de terceros.

Analizando los resultados del análisis referente a este proceso, se puede concluir que la administración de servicios de terceros no se la realiza adecuadamente, por lo que se entiende que es absolutamente necesario tomar medidas inmediatas a fin de evitar problemas, poniendo hincapié en los siguientes criterios:

Se debe identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad.

Además se recomienda identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener una efectiva entrega de servicios de forma segura y eficiente sobre una base de continuidad.

DS3: Administrar desempeño y capacidad.

Según los resultados obtenidos se concluye que la administración de desempeño y capacidad se la realiza de manera apropiada pero siempre es posible mejorar en los criterios donde no se ha conseguido un buen servicio.

La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere que se establezca un proceso de planeación para la revisión del desempeño y la capacidad

de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, con costos justificables, para procesar las cargas de trabajo acordadas.
Además brindar seguridad a los recursos de información que soportan los requerimientos del negocio para que estén disponibles de manera continua.

DS4: Garantizar la continuidad del servicio.

En referencia a este proceso y de acuerdo a los resultados obtenidos se puede determinar que se garantiza la continuidad de servicio pero debe poner énfasis en los siguientes criterios para obtener un mejor desempeño.
Se recomienda desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Además se debe probar dicho plan de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Se debe aplicar una estrategia para distribuir el plan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera.
Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio.

DS5: Garantizar la seguridad de los sistemas

Acorde a los resultados obtenidos se puede precisar que se garantiza la seguridad de los sistemas parcialmente y se debe poner énfasis en los siguientes criterios debido a que no se lo esta realizando en su totalidad.
Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.
Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa y además que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes.

Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas que estén implantadas.
Asegurar que la empresa cuente con medidas de prevención, detección y corrección a lo largo de toda la organización.

DS6: Identificar y asignar costos

De acuerdo a los resultados obtenidos se puede determinar que se cumple satisfactoriamente este proceso y que es preciso que se continúe tratándolo de la misma manera.

DS7: Educar y entrenar a los usuarios

Según los resultados obtenidos se puede establecer que este proceso tiene una adecuada aplicación por lo tanto se recomienda mantenerlo de esa forma.

DS8: Administrar la mesa de servicio y los incidentes

Se ha estipulado mediante la ejecución del proceso que la administración de la mesa de servicio y de incidentes no se la efectúa de manera apropiada, la respuesta a las consultas y problemas de los usuarios de TI no se lo realiza de manera oportuna y efectiva por lo que se recomienda poner énfasis en los siguientes puntos.
Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información.
Se deber establecer procedimientos de mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente y, si es adecuado, brindar soluciones alternas. Además establecer procedimientos para el monitoreo puntual de la resolución de consultas de los clientes.
Garantizar que la asignación de incidentes y el monitoreo del ciclo de vida permanecen en la mesa de servicios.
Emitir reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.

DS9: Administrar la configuración

Mediante el resultado de las encuestas se ha precisado que la administración de la configuración se la realiza de manera adecuada.

DS10: Administración de problemas

En lo que respecta a administración de problemas en la empresa, se pudo constatar que existe una adecuada administración, identificación y clasificación de lo mismos, no obstante se debe recalcar que es necesario la implantación pistas de auditoría adecuadas que permitan rastrear la causa raíz de todos los problemas reportados.

DS11: Administración de la Información

La empresa tiene establecidos métodos para la administración de la información, sin embargo se deben establecer procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios.

DS12: Administración del ambiente físico.

La administración del ambiente físico de TI en la empresa es la adecuada y es preciso mantenerlo de esa forma.

DS13: Administración de Operaciones

La empresa tiene establecido una adecuada administración de operaciones de TI, y es precio que la mantenga de esa forma.

***Resumen del dominio* Entregar y dar Soporte**

La entrega de los servicios requeridos que abarcan desde las operaciones tradicionales pasando por los aspectos de seguridad, integridad y continuidad hasta el entrenamiento es efectiva., por lo que se ha determinado que los costos de TI están siendo optimizados. Los procesos de soporte están establecidos para prestar servicios de una manera adecuada.

Por lo tanto se concluye que la gestión de este dominio es el adecuado y es preciso mantenerlo de esa manera.

MONITOREAR Y EVALUAR

ME1: Monitorear y evaluar el desempeño de TI.

En los resultados del análisis se puede ver claramente que el monitoreo y evaluación del desempeño de TI se cumple en gran parte, sin embargo presenta algunas falencias que deben ser tomadas en cuenta para una correcta administración.

Se debe definir indicadores de buen desempeño, reportes ordenados y oportunos de desempeño y tomar medidas claras cuando exista cualquier tipo de desviaciones.

ME2: Monitorear y evaluar el control interno.

La empresa se tiene implantado un proceso para monitorear y evaluar el control interno de TI, sin embargo no es el adecuado, se debe monitorear y reportar las excepciones de control, los resultados de las autoevaluaciones y revisiones por parte de terceros, así como también proporcionar seguridad en las operaciones y cumplir las leyes regulatorias aplicables.

ME3: Garantizar el cumplimiento regulatorio.

La empresa no tiene definido un proceso para garantizar el cumplimiento regulatorio, por ende se debe implantarlo inmediatamente, el mismo debe contener la definición de un reglamento de auditoria, independencia de los auditores, ética y estándares profesionales, planeación, desempeño del trabajo de auditoría, reportes y seguimientos a las actividades de auditoria.

ME4: Proporcionar Gobierno de TI.

Mediante la aplicación del proceso se pudo constatar que la empresa no tiene implantado un proceso para proporcionar gobierno de TI, así la implementación del mismo se debe llevar a cabo de inmediato.

El proceso debe contener un marco de trabajo de gobierno efectivo, incluyendo la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para de esta forma estar alineados de acuerdo a la estrategias y objetivo empresariales.

Resumen del dominio Monitorear y Evaluar

Mediante el análisis realizado se puede concluir que este dominio no se desempeña de forma adecuada y se debe tomar algunas medidas para corregir sus falencias.

Los procesos de TI son evaluados regularmente por su calidad y el cumplimiento con los requerimientos de control.

Los problemas y el desempeño son detectados a tiempo para evitar pérdidas económicas, retrasos en las entregas, etc.; el aseguramiento independiente no asegura que las áreas críticas están operando como se espera.

Las políticas, estándares y procedimientos de TI existente no garantizan que los requisitos legales y regulatorios se cubran de forma eficiente.

No se garantiza que los programas de inversión habilitados por TI de la empresa estén alineados con las estrategias y objetivos empresariales.

4.2.2 ANÁLISIS GENERAL

Los procesos de TI que se encuentran implantados en la empresa no son los suficientes para determinar que se encuentre en un óptimo desempeño. A continuación se cita los dominios en los cuales se presentan falencias:

- Planificar y Organizar
- Adquirir e Implementar
- Monitorear y Evaluar

El dominio Entregar y dar soporte no presenta falencias.

Entonces se concluye que para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren para ser administrados.

La carta emitida por la empresa GeoInfo (VER ANEXO 6) luego de revisar el informe técnico presentado, determina que el análisis de la aplicación del proceso en dicha empresa tiene un buen nivel de aceptación, puesto que las conclusiones presentadas reflejan la realidad de la empresa, y están concientes de que las falencias encontradas existen.

4.3EVALUACIÓN DEL PROCESO

Una vez obtenidos los resultados de la evaluación realizada a la empresa GeoInfo es importante analizar también que tan complicado o no resultó el manejo de este proceso y algunos aspectos de relevancia como los siguientes:

- Para poner en funcionamiento la aplicación del proceso deben interactuar mínimo dos personas, quien evalúa el proceso sobre la empresa, quien conoce todo el contenido de las operaciones de TI.
- Cuando se va aplicar el proceso, es necesario considerar el tipo de empresa, pero en el desarrollo del proceso se ha determinado que será de uso exclusivo para empresas desarrolladoras de software.
- El proceso fue de mucha utilidad para detectar aspectos relativos al mejoramiento de las operaciones de TI.
- Los resultados de la evaluación del proceso respecto al cumplimiento o no de ciertos aspectos de importancia, serán aplicados, para el mejoramiento del desempeño de las operaciones de TI.
- La utilización de este proceso es independiente de los autores ya que sirve de forma genérica para todas las empresas desarrolladoras de software que deseen controlar la calidad de sus procesos. Y seria mucho más fácil de utilizar a quien tenga un básico conocimiento de COBIT 4.0.
- Para el responsable de las operaciones de TI este proceso es de mucha utilidad, ya que optimizará el tiempo invertido en el control de los procesos, con la autenticidad de que cada punto de revisión esta regido sobre el estándar COBIT 4.0.

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

5.1CONCLUSIONES

Para el mejor desempeño de las operaciones de TI en empresas desarrolladoras de software, es precisa la evaluación de las mismas, es por eso que se ha planteado un proceso para brindar al evaluador un apoyo rápido y concreto, ya que este proceso se ajustan solo a dichas empresas. El proceso se ha planteado en base a que en la actualidad las organizaciones ya están interesadas en la aplicación del marco de trabajo de TI de COBIT 4.0, aunque se observó que en las diversas empresas desarrolladoras de software no se tenía conocimiento del marco de referencia utilizado. Por lo tanto, puede este proyecto convertirse en una guía práctica, específicamente para empresas desarrolladoras de software.

La evaluación de las operaciones de TI es importante en la toma de decisiones, ya que permite determinar el estado actual de la empresa, muestra los aspectos que se están desarrollando adecuadamente y los que no también. Para nuestro caso se tuvo como pilar fundamental un estudio estadístico respaldado con documentos obtenidos de manera formal, acudiendo a las empresas competentes, por tanto podríamos concluir que el uso de la estadística fue de vital importancia y dió las pistas necesarias para realizar el proceso, por tanto se debe rescatar su valor ya que ha permitido establecer criterios que ayudaron a especificar que aspectos necesitan ser reforzados en las empresas de nuestro medio, cumpliendo con el objetivo de fusionar la teoría existente con nuestra realidad.

Para aplicar este proceso no se necesita una alta inversión económica ni mucho tiempo para la evaluación, pero si es necesario que el encargado de realizar la evaluación tenga un total conocimiento de los procesos de TI que se realizan en la empresa, además que tenga previos conocimientos del estándar COBIT 4.0. La interpretación de resultados que se presenta en este proceso ha sido basado en recopilaciones de investigaciones realizadas en distintas tesis, y el estándar COSO.

Esta investigación puede servir como base para el desarrollo de nuevas investigaciones debido a que COBIT se actualiza constantemente.

Después del análisis realizado a las empresas desarrolladoras de software de Quito, se puede concluir que aunque la mayoría de las empresas encuestadas consideran importante la administración de las operaciones de TI, no tienen una definición adecuada de las mismas.

5.2RECOMENDACIONES

Recomendamos la aplicación de este proceso, ya que es de fácil comprensión y utilización, debido a que presenta los pasos que debe seguir el evaluador, así como también, presenta cuestionarios que ayudarán al evaluador en la recolección de la información.

Es recomendable que este proceso cuente con la aprobación y respaldo de parte de las autoridades competentes dentro de la empresa, al igual que resulta fundamental que sea aplicada por un profesional que posea ciertas características como: transparencia, conocimiento de las operaciones de TI e imparcialidad, con el objetivo de que los resultados obtenidos sean ciertamente valiosos y que presenten un verdadero aporte, buscando siempre el mejoramiento continuo.

Es recomendable realizar evaluaciones periódicas para tener una visión acertada de las falencias sustentadas en el desempeño de las operaciones de TI, para lo cual se podría desarrollar una aplicación tomando en cuenta nuestro proceso como base, aplicándolo a la realidad de una empresa y adaptándolo a sus necesidades.

Es probable que incluso profesionales olviden la existencia de normas, estándares, metodologías y leyes, dada la necesidad de realizar este trabajo de manera rápida, pero esto realmente constituye un perjuicio en innumerables sentidos, es siempre importante realizar cualquier trabajo profesional con el respaldo oportuno de aquellos estudios que fundamentan las bases de cualquier campo de la ciencia.

El auditor, basándose en un análisis de los resultados, debe presentar recomendaciones razonables y acordes con la situación de la empresa en la cual se realice la aplicación del proceso.

GLOSARIO DE TÉRMINOS

Actividad: Las medidas principales tomadas para operar el proceso COBIT.

Administración de la configuración: El control de cambios realizados a un conjunto de componentes de la configuración a lo largo del ciclo de vida del sistema.

Administración del desempeño: La capacidad de administrar cualquier tipo de medición incluyendo mediciones de empleados, equipo, proceso, operativas o financieras. El término denota un control de ciclo cerrado y la vigilancia periódica de la medición.

Arquitectura de la información: Ver arquitectura de TI.

Arquitectura de TI: Un marco integrado para evolucionar o dar mantenimiento a la TI existente y adquirir nueva TI para alcanzar las metas estratégicas y de negocio de la empresa.

Arquitectura empresarial: Mapa de rutas tecnológicas orientada al negocio para el logro de las metas y objetivos de negocio.

Arquitectura empresarial para TI: Respuesta en la entrega de TI, provista por procesos claramente definidos usando sus recursos (aplicaciones, información, infraestructura y personas).

Atención al usuario: El único punto de contacto dentro de la organización de TI para los usuarios de los servicios prestados por TI.

CEO: Director ejecutivo.

CFO: Director financiero.

CIO: Director de información [algunas veces Director de Tecnología (CTO, por sus siglas en Inglés)].

Cliente: Una persona o una entidad externa o interna que recibe los servicios empresariales de TI.

Continuidad: Prevenir, mitigar y recuperarse de una interrupción. Los términos "planear la reanudación del negocio", "planear la recuperación después de un desastre" y "planear contingencias" también se pueden usar en este contexto; todos se concentran en los aspectos de recuperación de la continuidad.

Control: Las políticas, procedimientos, practicas y estructuras organizacionales diseñadas para proporcionar una garantía razonable de que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados.

Control general: También control general de TI. Un control que se aplica al funcionamiento general de los sistemas de TI de la organización y a un conjunto amplio de soluciones automatizadas (aplicaciones).
Control Interno: Las políticas, procedimientos, practicas y estructuras organizacionales diseñadas para brindar una garantía razonable de que los objetivos del negocio se alcanzarán y de que los eventos indeseables serán prevenidos o detectados y corregidos.

Control preventivo: Un control interno que se usa para prevenir eventos indeseables, errores u otras ocurrencias que pudieran tener un efecto material negativo sobre un proceso o producto final, de acuerdo a la organización.

COSO: Comité de organizaciones patrocinadoras de la comisión Treadway. Estándar aceptado a nivel internacional para el gobierno corporativo. Ver *www.coso.org*.

Desempeño: La implantación real o el logro de un proceso.

Diccionario de datos: Un conjunto de meta-datos que contiene definiciones y representaciones de elementos de datos.

Diccionario de datos empresarial: El nombre, tipo, rango de valores, fuente, sistema de registro, y autorización de acceso para cada elemento de datos utilizado en la empresa. Indica cuáles programas aplicativos usan esos datos, de tal forma que cuando se contemple una estructura de datos, se pueda generar una lista de los programas afectados.

Directriz: La descripción de un modo particular de lograr algo, la cual es menos prescriptiva que un procedimiento.

Dominio: Agrupación de objetivos de control en etapas lógicas en el ciclo de vida de inversión en TI

Empresa: Un grupo de individuos que trabajan juntos para un fin común, por lo general dentro del contexto de una forma organizacional, como una corporación agencia pública, entidad de caridad o fondo.

Estándar: Una práctica de negocio o producto tecnológico que es una práctica aceptada, avalada por la empresa o por el equipo gerencial de TI. Los estándares se pueden implantar para dar soporte a una política o a un proceso, o como respuesta a una necesidad operativa. Así como las políticas, los estándares deben incluir una descripción de la forma en que se detectará el incumplimiento.

Evaluación por comparación (Benchmarking): Un proceso utilizado en administración, en particular en la administración estratégica, en el cual las compañías evalúan varios aspectos de sus procesos de negocio con respecto a las mejores prácticas, por lo general dentro de su propia industria.

Gobierno: El método por medio del cual una organización es dirigida, administrada o controlada.

Gráfica RACI: Ilustra quién es responsable, quién debe rendir cuentas, a quién se debe consultar e informar dentro de un marco de trabajo organizacional estándar.

Incidente: Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o una reducción de la calidad de ese servicio (alineado a ITIL).

Infraestructura: La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.

ITIL: Librería de Infraestructura de TI de la Oficina de Gobierno Gubernamental del Reino Unido (OGC).Un conjunto de lineamientos sobre la administración y procuración de servicios operativos de TI.

KGI: Indicador clave de meta.

KPI: Indicador clave de desempeño.

Madurez: Indica el grado de confiabilidad o dependencia que el negocio puede tener en un proceso, al alcanzar las metas y objetivos deseados.

Marco de control: Una herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte.

Marco de trabajo: Ver Marco de control.

Métrica: Un estándar para medir el desempeño contra la meta.

Modelo de madurez de la capacidad (CMM): El modelo de madurez de la capacidad para software (CMM), del Instituto de Ingeniería de Software (SEI), es un modelo utilizado por muchas organizaciones para identificar las mejores prácticas, las cuales son convenientes para ayudarles a evaluar y mejorarla madurez de su proceso de desarrollo de software.

Objetivo de control: Un estatuto del resultado o propósito que se desea alcanzar al implantar procedimientos de control en un proceso en particular.

Organización: La manera en que una empresa está estructurada.

Plan estratégico de TI: Un plan a largo plazo, Ej. con un horizonte de tres a cinco años, en el cual la gerencia del negocio y de TI describen de forma cooperativa cómo los recursos de TI contribuirán a los objetivos estratégicos empresariales (metas).

Plan de infraestructura tecnológica: Un plan para el mantenimiento y desarrollo de la infraestructura tecnológica.

Plan táctico de TI: Un plan a mediano plazo, Ej. con un horizonte de seis a dieciocho meses, que traduzca la dirección del plan estratégico de TI en las iniciativas requeridas, requisitos de recursos y formas en las que los recursos y los beneficios serán supervisados y administrados

PMBOK: Cuerpo de conocimiento de administración de proyectos, un estándar para administración de proyectos desarrollado por el Instituto de Administración de Proyectos (PMI).

PMO: Director de administración de proyectos.

Política: Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos gerenciales de la empresa. Además del contenido de la política, esta debe describir las consecuencias de la falta de cumplimiento de la misma, el mecanismo para manejo de excepciones y la manera en que se verificará y medirá el cumplimiento de la política.

Portafolio: Una agrupación de programas, proyectos, servicios o activos seleccionados, administrados y vigilados para optimizar el retorno sobre la inversión.

Problema: Causa subyacente desconocida de uno o más incidentes.

Procedimiento: Una descripción de una manera particular de lograr algo; una forma establecida de hacer las cosas; una serie de pasos que se siguen en un orden regular definido, garantizando un enfoque consistente y repetitivo hacia las actividades.

Proceso: Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma las entradas provenientes de un número de fuentes, incluyendo otros procesos, manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, propietarios responsables, roles claros y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.

Proceso de negocio: Ver Proceso.

Programa: Una agrupación estructurada de proyectos independientes que incluye el alcance completo del negocio, del proceso, de las personas, de la tecnología y las actividades organizacionales que se requieren (tanto necesarias como suficientes) para lograr un resultado de negocios claramente especificado.

Programa aplicativo: Un programa que procesa los datos del negocio a lo largo de las actividades, tales como la captura, actualización o consulta de datos. Contrasta con los programas de sistemas, tales como un sistema operativo o un programa de control de redes, y con los programas utilitarios, tales como *copiar (copy)* o clasificar (*sort).*

Propietarios de datos: Individuos, por lo general gerentes o directores, que tienen la responsabilidad de la integridad, el uso y el reporte preciso de los datos computarizados.

Proveedor de servicios: Organización externa que presta servicios a la organización.

Proyecto: Un conjunto estructurado de actividades relacionadas con la entrega de una capacidad definida a la organización (la cual es necesaria, aunque no suficiente para lograr un resultado de negocios requerido) con base en un calendario y presupuesto acordado.

QMS: Sistema de administración de la calidad. Un sistema que describe las políticas y procedimientos necesarios para mejorar y controlar los distintos procesos que al final conducirán a un desempeño mejorado del negocio.

Riesgo: El potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia.

Segregación/separación de tareas: Un control interno básico que previene y detecta errores o irregularidades por medio de la asignación a individuos diferentes, de la responsabilidad de iniciar y registrar las transacciones y la custodia de los activos.

SDLC: Ciclo de vida del desarrollo de sistemas. Las fases utilizadas en el desarrollo o adquisición de un sistema de software. Las fases típicas incluyen al estudio de factibilidad, el estudio de los requerimientos, la definición de requerimientos, el diseño detallado, la programación, las pruebas, la instalación y la revisión post-implantación.

SLA: Acuerdo de nivel de servicio. Acuerdo por escrito entre un proveedor de servicios y los usuarios del cliente, el cual documenta los niveles de servicio acordados para un servicio prestado.

TI: Tecnología de información.

Usuario: Una persona que utiliza los sistemas empresariales.

Universo:

BIBLIOGRAFÍA

PAGINAS WEB

El planteamiento del problema de la investigación.

http://www.integrando.org.ar/investigando/el_problema.htm

Muestreo Aleatorio

http://www.bioestadistica.uma.es/libro/node88.htm

Análisis de Resultados

http://www.asofis.org.mx/mejores_practicas/COSO.pdf

COSO departamento de auditoría de la EPN

COBIT 4.0 Objetivo de Control, Directrices Gerenciales y Modelos de Madurez.

http://www.isaca.org/Template.cfm?Section=Downloads10&CONTENTID=39287&TEMPLATE=/ContentManagement/ContentDisplay.cfm. Abril 2007.

IT Governance Institute

www.itgi.org

TESIS

MANTILLA Salome, PAZOS Xavier; Guía para la aplicación de las técnicas de auditoria informática en la empresas de Quito; Quito, EPN. FIS 2003

DELGADO María, LIZANO Irina; Auditoria de los Procesos Software de una empresa de Servicios Informáticos; Quito, EPN. FIS 2003

MATUTE Margarita, CAIZA Angélica; Evaluación de riesgos en empresas desarrolladoras de software utilizando la herramienta MSAT; Quito, EPN. FIS 2007

VELASTEGUI Talina; Análisis de la gestión de las Tecnologías de la Información en la Unidad de Gestión Informática de la EPN; Quito, EPN. FIS 2007

LIBROS Y ESTÁNDARES

GALINDO DE LA TORRE Edwin. Estadística para la Administración y la Ingeniería. Primera edición. Gráficas Mediavilla Hnos. Quito – Ecuador. 1999.

IT Governance Institute. COBIT 4.0 Objetivo de Control, Directrices Gerenciales y Modelos de Madurez. Glanser Services. 2007

COBIT MARCO REFERENCIAL; 3a Edición. Emitido por el Comité Directivo de COBIT y El IT Governance Institute 2001

ANEXOS

ANEXO 1: LISTADO DE EMPRESAS DESARROLLADORAS DE SOFTWARE

LISTADO DE EMPRESAS DESARROLLADORAS DE SOFTWARE

	NOMBRE DE LA COMPAÑÍA	TELEF
1	COMPUSUD CA	2468426
2	SANCHO ARIAS C LTDA	2909007
3	OTCATNOC S.A.	2247208
4	INFORMACION TECNOLOGICA DEL ECUADOR LUXEINFORM S.A.	2560866
5	CONSULTORES DE SISTEMAS INTEGRALES CONSULTSISTEM CIA. LTDA.	2450147
6	GENNASSIS CIA. LTDA.	2250279
7	INTERLANCOMPU CIA. LTDA.	2502269
8	NESTOR MARROQUIN N.M.C. RESEARCH CIA. LTDA.	2650431
9	INSOFT INFORMATICA Y SOFTWARE CIA. LTDA.	2551362
10	ABACUSASESORES S.A.	2268348
11	SOLUCIONES TECNOLOGICAS GEOINFO CIA. LTDA.	2220191
12	ESERV EXPERT SERVICES DEL ECUADOR S.A.	2986653
13	WEBMARKER S.A.	2986440
14	ASESORIA TECNICA Y SERVICIOS GUERRERO & GUERRERO CIA. LTDA.	953514
15	SOLUCIONES DE ALTA TECNOLOGIA SYSDATA CIA. LTDA	2469058
16	CAYMANSYSTEMS CIA. LTDA	2221178
17	ADVENTURE INFO CIA. LTDA.	259792
18	CERTSOFT ASESORES CIA. LTDA.	2527565
19	ACTIVA TECNOLOGIA INFORMATICA CIA. LTDA	2278032
20	NEGOCIOS, COMERCIO, Y DISEÑO EN LA RED S.A NETCODE	2551362
21	INTERINFORMATICA S.A.CENTRO DE EDUCACION INFORMATICA GERENCIAL	2273398
22	KZE COMUNICACION AUDIOVISUAL CIA. LTDA.	3238613
23	PARTNERSOFT CIA. LTDA	2652554
24	ATMGLOBSERV C.A	2273749
25	PC & PC SOLUTIONS CIA. LTDA.	2236536
26	ASISTENCIA TECNICA Y COMERCIAL ASISTECOM CIA. LTDA.	2265001
27	GLOBALWARE SOLUCIONES INFORMATICAS GLOBALES S.A.	2272779
28	TRIBAL D.C.M. CIA. LTDA	2559998
29	SOLUCIONES INTEGRALES OMNISOFT CIA. LTDA	3342688
30	CINNET INGENIERIA DE REDES Y SISTEMAS CIA. LTDA.	2546069
31	INTEGRATED SOLUTIONS CORP S.A	2261630
32	MR CONSULTING AND INFOSOLUTIONS CIA. LTDA.	3441297
33	OBJETIVOS, ESTRUCTURA, PROCEDIMIENTOS Y AUTOMATIZACION OEPA S.A	2800458
34	BROWSE ECUADOR CIA. LTDA.	2569023
35	TELEAUTOMATISMOS V&P S.A.	2258321
36	TECHNOLOGY REAL EXPERIENCE T-REX DEL ECUADOR CIA. LTDA.	2558268
37	SQO PROFESIONALES ASOCIADOS CIA. LTDA	2536573
38	ALPHASOFT S.A.	2354165
39	SOLUTIONETECH DEL ECUADOR CIA. LTDA.	3237015
40	CORPORACION TECNOLOGIA DE LA INFORMACION SOLUTANDI CIA. LTDA.	2232579
41	PRODUCTIVIDAD & TECNOLOGIA SERVICES S.A. PRODUCSERTEC	2236798
42	SOLUCIONES G CUATRO DEL ECUADOR ECUCUATRO S.A.	2250116
43	TELEMATICA BUSINESS COMPANY TEBUSCO S.A.	2891557
44	MOVILCONTROL TECHNOLOGY CIA. LTDA.	2239007
45	SIDSOLUTION CIA. LTDA.	2242574

		5
46	DAYSCRIPT ECUADOR S.A.	2460007
47	EMPRESA INTEGRAL DE INFORMATICA S.A. EMPRINFOR	2480452
48	SISTEMAS MEDICOS INFORMATICOS INFOMEDICS CIA. LTDA.	2230278
49	RFCENKLAVE GESTION TECNOLOGICA E INNOVACION CIA. LTDA.	2468369
50	MERCADOLIBRE ECUADOR S.A.	2251319
51	INTELIGENCIA & NEGOCIOS INTELNEGSA S.A.	2434346
52	DGTX INTERNACIONAL S.A.	2904560
53	SISVIRTUAL SISTEMAS VIRTUALES CIA. LTDA.	2528261
54	DIGIWARE SEGURIDAD DEL ECUADOR S.A.	2460867
55	LOGGISERVICES S.A.	2245830
56	CORPODEPRO CORPORACION PARA EL DESARROLLO Y PROMOCION UNIVERSAL S.A.	3281297
57	EB S.A.	2444071
58	NITESTAR DE LATINOAMERICA C.A.	2270925
59	ASESORIA Y COMERCIALIZACION DE SERVICIOS TECNOLOGICOS EMSERTEC S.A.	2553553
60	TATASOLUTION CENTER S.A.	2562680
61	SIREDCOM S.A. SOLUCIONES INFORMATICAS Y REDES DE COMUNICACION	2974597
62	LATINTAX SOFTWARE DEL ECUADOR S.A.	2266110
63	SYSDEV MOBILE TECH ECUADOR S.A.	2430581
64	ITRICE, INGENIERIA EN TELECOMUNICACIONES, REDES, INFORMATICA Y CONTROL ELECTRONICO CIA. LTDA.	3262558
65	DATACTIVA S.A.	2444002
66	BSGCONSULTING CIA. LTDA.	2981764
67	COMPAÑIA DE TELECOMUNICACIONES TELGICOM CIA. LTDA.	2667525
68	MAGEFI SISTEMAS ASESORIA Y NEGOCIOS MAGEFI CIA. LTDA.	2467030
69	SITCOBTECNO CIA. LTDA.	3203400
70	XYPREPAGO S.A.	6001820
71	QOS TECHNOLOGIES CIA. LTDA.	2241605
72	M.R.U. PRODUCTOS DE LABORATORIO CIA. LTDA.	
73	FAPASAGLOBAL CIA LTDA	3313329
74	ISTH INTEGRANDO SOLUCIONES TECNOLOGICAS CIA. LTDA.	3020815
75	FICHTNER GMBH & CO. KG	2506866
76	GFKECUADOR S.A. INVESTIGACION ESTRATEGICA	6001222
77	SERVICIOS INFORMATICOS PEKESCORP S.A.	2664092
78	FINANWARE CIA. LTDA.	2532475
79	BLUE LIZARD GAMES ECUADOR S.A.	2895031
80	ADVANTLOGIC ECUADOR S.A.	22239896
81	SISTEMAS DE INFORMACION DECISION COMPAÑIA ANONIMA	2262550
82	GRUPO MICROSISTEMAS JOVICHSA S. A.	2923500
83	CPUSYSTEM C LTDA	2522865
84	DINSISTEMAS C LTDA	3228450
85	SIGNUM CIA LTDA	2501470
86	SISTEMAS GUIA S.A. GUIASA	2491842
87	EXECSISTEMAS CIA. LTDA.	2415568
88	TAND-G DEL ECUADOR S.A.	2550145
89	UNICODE S.A.	2245324
90	TEOPSIS TECNOLOGIA, OPTIMIZACION Y SISTEMAS S.A.	2924421
91	GRUPO TECNOLOGICO MAINTQUITO S.A.	2500921
92	GRUPOCONTEXT S.A.	26001232

93	RESPUESTAS DE ULTIMA TECNOLOGIA RESULTSYS CIA. LTDA.	2252440
94	SOLSOFT CIA. LTDA.	2070695
95	ELECTRIFORSYSTEMS, EIS C. LTDA.	2442515
96	SISTRAN ANDINA SISTRANDI CIA. LTDA.	2237170
97	SMARTTEC CIA. LTDA.	2263439
98	DBASYSTEMATICA ECUADOR CIA. LTDA.	2451278
99	KRUGERCORPORATION S.A.	0224477 82
100	GENERACION SISTEMAS SUMISISTEMS CIA. LTDA.	2242488
101	REDPARTNER S.A.	2540000
102	PROTELCOTELSA S.A.	2430992
103	SOLUCIONES INFORMATICAS DEL FUTURO SIFUTURO S.A.	2547585
104	PAMINCE CIA. LTDA.	2610770
105	WEBCONEXION S.A.	2040491
106	MBASOFTWARE SOLUTIONS CIA. LTDA.	2508856
107	LOHNBERG SYSTEMS S.A.	2237373
108	SISTEMAS DE INFORMACION GEOGRAFICA Y COMERCIO ELECTRONICO NETGIS S.A.	2501479
109	DATANET S.A.	2257448
110	NEKKAR S.A.	2449943
111	INGENIERIA Y DESARROLLO DE SISTEMAS INDESIS CIA. LTDA.	2527882
112	INTEGRADORSST SERVICIOS, SOLUCIONES Y TECNOLOGIA S.A.	2560129
113	BARLALCAS S.A.	2468717
114	MAXIMA RIFLOSAN SISTEMAS INFORMATICOS S.A.	2251921
115	LOGICIEL CIA. LTDA	2523413
116	GREENTRACONS GREEN SOFT CIA. LTDA.	2227461 9
117	MASCOMMERCE C. LTDA.	2527123
118	M.Q.R. AUDITORIA & INGENIERIA INFORMATICA S.A.	2270010
119	SOLDENEG SOLUCIONES DE NEGOCIOS CIA. LTDA.	2555207
120	AMATECH CIA. LTDA	2923058
121	VIMEWORKS CIA. LTDA.	2237784
122	DESARROLLO DE SISTEMAS Y VENTAS DE COMPUTADORES SYSTEM HOME S.A.	2441142
123	INTERMIX S.A.	2903853
124	BAYTEQ CIA. LTDA.	2505002
125	MECH & TECH INGENIERIA Y TECNOLOGIA CIA. LTDA	2498990
126	GARNICORP S.A.	2565650
127	SMART ADVICE S.A. ASESORAMIENTO Y DESARROLLO DE SISTEMAS	2261231
128	PREMIUMLATINO S.A.	2454211
129	SMARTKEY CIA. LTDA.	2244159
130	LEE TELECOMUNICACIONES S.A	2226451
131	ECUABUXIS S.A	2234029
132	SYSTEMS DEVELOPMENT CONSULTANTS SDCONSULT CIA. LTDA.	2267423
133	GIGADIGITAL S.A.	2921007
134	VENTURE VENTI CIA. LTDA.	2545699
135	COMERCIAL GRIFFMETAL S.A.	2567263
136	NICOSISTEM CIA. LTDA	2456559
137	FALCON SYSTEMS S.A. SISTEMAS INFORMACION SERVICIOS	2418726
138	INTERBASES INTEGRACION DE BASES DE DATOS IBADATA CIA. LTDA.	2230247
139	RIVERA ZEPEDA CIA. LTDA	2453200
140	O.C.M. COMPUTERS OCAÑA MORA COMPUTADORES CIA. LTDA	2545243

141	QUALITYSOFT INNOVATIVE SOLUTIONS Q.S.S. CIA. LTDA	2906618
142	COMPAÑIA SONUEM SOLUCIONES PARA EL NUEVO MILENIO CIA. LTDA	2656517
143	COMPUTER BUSINESS MANAGEMENT ASOCIADOS C.B.M. CIA. LTDA	2558391
144	OPTIMSOFT SOFTWARE & HARDWARE CIA. LTDA.	2292834
145	THESYS TECHNOLOGIES CIA. LTDA	2433963
146	OBJECTEL CIA. LTDA	2951513
147	ALPHA TECHNOLOGIES CIA. LTDA	22814291
148	EASYSOFT S.A.	2435200
149	LOGICA INTERNACIONAL LOGICAL CIA. LTDA.	2438513
150	LIONEL SIERO INTERACTIVE SOFTWARE CIA. LTDA.	2501199
151	DESAROLLO DE SISTEMAS Y TELECOMUNICACIONES DESYTEL CIA. LTDA	2548226
152	MULTIMEDIASHOQ CIA. LTDA	2253531
153	ICAP DEL ECUADOR S.A	33330900
154	APOCALIPSIS SOLUTIONS CIA. LTDA	2528667
155	SISTEMAS DE PROCESAMIENTO DE DATOS SYSDATEC DEL ECUADOR S.A.	2907161
156	ICOMS INTEGRAL COMPUTING SYSTEMS CIA. LTDA	09804319
157	DB WARE CIA. LTDA.	2529932
158	NETEC NEGOCIOS Y TECNOLOGIA S.A.	2551117
159	QMC SYSTEMS INGENIERIA INFORMATICA CIA. LTDA	2271835
160	CYBERSOFT CIA. LTDA.	2465517
161	VISION EMPRESARIAL VISUALTEK CIA. LTDA	2236486
162	INGENIERIA DE SISTEMAS IDS-ECUADOR CIA. LTDA.	2527882
163	SOFT WAREHOUSE S.A.	22923211
164	MALTERCIO.COM CIA. LTDA.	2269260
165	LIFE COMPONENT CIA. LTDA.	2256867
166	AEROTECNOLOGIA CIA. LTDA.	2473524
167	SCALAR CONSULTING CIA. LTDA.	22410489
168	TECSINFO S.A	2223214
169	CIRVZ DEL ECUADOR CIA. LTDA.	2658588
170	DINAMA APLICACIONES MOVILES S.A	2986440
171	EQTEK S.A.	2261640
172	MINDSOFT CIA. LTDA	2447861
173	PACIFIC SOFTWARE S.A	2460754
174	WEB SYSTEMS SISTEMAS INTERACTIVOS CIA. LTDA	2433604
175	BRA SOLUTIONS CIA. LTDA	2242700
176	DESAROLLO DIGITAL DESDIG S.A	2527540
177	E-DENTALSYS ECUADOR S.A.	022260170
178	SEREDUTEK S.A. SERVICIOS EDUCATIVOS TECNOLOGICOS	2549800
179	EMSOLNEG EMPRESA SOLUCIONES Y SERVICIOS CIA. LTDA.	2263726
180	INDUSNAV & DEFENSAIR REPRESENTACIONES S.A.	2901308
181	INFOHOST C.A.	2903651
182	AEROSOFTWARE CIA. LTDA.	2504258
183	TECNOLOGIA INTERNACIONAL PARA EL ECUADOR INTECAVANT S.A.	2904658
184	INTERNET TECHNOLOGIES FINANTECH S.A.	2923211
185	GREEN TECHNOLOGIES ASESORIA INFORMATICA S.A.	2905735
186	PROGRAMAS INFORMATICOS INFOPRO S.A.	3341341
187	BUSINESSMIND S.A.	6002855

188	SIFIZSOFT S.A.	2448034
189	DIGITALTEAM S.A.	2544577
190	KEY WORLD SISTEMAS S.A.	2552612
191	SISTEMA INTEGRADO DE EMPRESARIOS SISINTEMP CIA. LTDA.	2486305
192	SMARTWORK S.A.	2557353
193	BIGBRANCH S.A.	2261277
194	BIOMETRIKA S.A.	2524-201
195	SOLTEGIN SOLUCIONES TECNOLOGICAS S.A.	2431558
196	INFORMATICS SOLUTIONS & SERVICIOS EMPRESARIALES SINSEM S.A.	2504258
197	ACTIVATEC TECNOLOGIA ACTIVA CIA. LTDA.	2346116
198	SOPORTE LIBRE FREESUPPORT CIA. LTDA.	2568068
199	TECNOLOGIA LINCOLN LIBERTY GROUP CIA. LTDA.	22546884
200	COMERCIALIZADORA ENTERPRISE SOFTWARE SOLUTIONS ECUADOR CIA. LTDA.	2508856
201	ZONA INFORMATICA EXCELTECH CIA. LTDA.	2409167
202	GLOBALEQUIS MANAGEMENT SOLUTIONS S.A.	2433209
203	IBCORP TECHNOLOGIES S.A.	2398842
204	EMERGESOFT CIA. LTDA.	2530391
205	BUILDERSOLUTIONS SOLUCIONES INFORMATICAS CIA. LTDA.	2435014
206	NUEVOS DESARROLLADORES NDEVELOPER CIA. LTDA.	2568068
207	BALAREZO & CONSULTORES DE TECNOLOGIA Y PROCESOS CIA. LTDA.	2551507
208	PROINFECUA PROYECTOS DE INFORMATICA DEL ECUADOR C.A.	2508059
209	REDSOLUCIONES S.A.	2457525
210	ECLICKSA SERVICIOS Y ASESORIA S.A.	2509893
211	MAXINFO CIA. LTDA.	96213927
212	TECNOLOGIAS SAZECUADOR CIA. LTDA.	023238031
213	SERVICIOS ROEBIN CIA. LTDA.	2209797
214	LINGUATEK CIA. LTDA.	2445532
215	OPENVISION S.A.	2455585
216	CEREBRO PERIFERICO SDS CIA. LTDA.	2490288
217	AXG LIMITED	2288029
218	CORPORACION QUEHACEREC S.A.	2269190
219	TECNOLOGIA URBANA S.A. URBATECH	2223057
220	PROGRAMAS Y SOFTWARE ACADEMICOS ANDINOS PROGRANDINOS S.A.	2501500
221	EDISOFT DESARROLLO DE SISTEMAS CIA. LTDA.	022553768
222	GLOBALDEV INFORMATICA Y TELECOMUNICACIONES CIA. LTDA.	2278233
223	FIABLE. NET INVESTIGACION DESARROLLO Y ADMINISTRACION DE EMPRESAS CIA. LTDA.	2432902
224	SERVICIOS INTEGRADORES DE MENSAJERIA DE TEXTO Y TECNOLOGIA MISIVACORP S.A.	2256750
225	BUSINESS LAND S.A	2923805
226	ALSAFLEX COMPANY S.A.	2228857
227	METASOURCE S.A.	2242626
228	DREAMSOFT ECUADOR CIA. LTDA.	2478484
229	CODIGO EMPRESARIAL DEL ECUADOR ECUACODEM S.A.	2439217
230	TRANSTELFON S.A.	2223222
231	ACCESOS ECUADOR ACCECUADRO CIA. LTDA.	2436069
232	GEOINT CIA. LTDA.	2242197
233	TELLER SOLUTIONS CIA. LTDA.	2331424

234	AGRESSGROUP S.A.	2502332
235	SOLUCINT SOLUCIONES INTELIGENTES CIA. LTDA.	0233174 32
236	AFIGETEC CIA. LTDA.	2227352
237	SEVENTEENMILE S.A.	2921012
238	SOLINTECE CIA. LTDA.	2551991
239	PENITUS SOLUTIONS CIA. LTDA.	2269296
240	PROTECOMOVIL S.A.	2560600
241	MOBILE INTERNET GROUP LATINOAMERICA S.A. MIGECUADOR	2292244 6
242	REFUNDATION CONSULTING ASESORIA INFORMATICA CIA. LTDA.	2568068
243	EMAGIC NEGOCIOS ELECTRONICOS S.A.	2908299
244	ECUSOLID S.A.	2455858
245	SOLULASER SOLUCIONES LASER S.A.	2269968
246	HSB SOFTECUADOR CIA. LTDA.	2040991
247	SOFDECISION SOFTWARE & SISTEMAS CIA. LTDA.	3227554
248	IMPORTADORA EXPORTADORA SHIYAMIK CIA. LTDA.	2338688
249	IBEGTA GLOBAL TECHNOLOGY ALLIANCE S.A.	2223659
250	BUSINESS TECH CIA. LTDA.	2242120
251	ISOFTEC INGENIERIA EN SOFTWARE Y TECNOLOGIA INFORMATICA CIA. LTDA.	0229066 37
252	ISEDEC INFORMATICA Y SEGURIDAD ELECTRONICA DEL ECUADOR CIA. LTDA.	2346880
253	DYNAMIC MODULAR SYSTEM ECUADOR S.A.	2226229
254	CONSORCIO DE ASESORES Y SERVICIOS OUTSOLUTIONS CIA. LTDA.	2903240
255	MAGMASOFT INNOVANDO TECNOLOGIA CIA. LTDA.	2568068
256	NOVARED SYSTEMS SRB S.A.	2565050
257	HIDROMAGAS S.A.	2265180
258	DATABANK MANAGEMENT KNOWLEDEWARE SOLUTIONS LIMITADA, DATABANK MKS LTDA.	2555913
259	BUPARTECH S.A.	2249532
260	HEEDAE KIM IMPORT EXPORT CIA. LTDA.	0987276 84
261	ANDESOFT INTERNATIONAL CIA. LTDA.	2270144
262	SHS DEL ECUADOR CIA. LTDA.	2974397
263	MARKETBRAND ESTRATEGIAS PARA MERCADEO EN MEDIOS DIGITALES CIA. LTDA.	2609565
264	NETWORK SOLUCIONES & WEB COMUNICACIONES NETWEBCO S.A.	2222044
265	SAGSOH CIA. LTDA.	2239215
266	WEBARED INTERNET SOLUTIONS ECUADOR S.A.	2220550
267	FORTISIDERIS CIA. LTDA.	2529157
268	ASITECNO ASESORIA EN SERVICIOS DE INTERNET Y TECNOLOGIA CIA. LTDA.	2548313
269	JMS VALENCIA CIA. LTDA.	0328437 23
270	ATM GLOBAL SERVICES INTERNACIONAL C.A.	2450896
271	SOLUCIONES INFORMATICAS INFOTECNOS CIA. LTDA.	2600865
272	GLOBALX LOGISTIC SOLUTIONS GXLS S.A.	2433209
273	SERATVOIP S.A. SERVICIOS DE ADMINISTRACION DE TECNOLOGIA	2277300
274	SOLUCIONES TECNOLOGICAS CASTILLO & QUIROZ CIA. LTDA.	2074083
275	DISISOT DISEÑO DE SISTEMAS Y SOLUCIONES TECNOLOGICAS CIA. LTDA.	2438719
276	NUWAYSOFT CORP CIA. LTDA.	2403466
277	T&G TECNOLOGIA Y GESTION - SERVICIOS CIA. LTDA.	2560866
278	SISTEMAS Y SOLUCIONES ANDINAS ANDISISTEMS S.A.	2506866
279	AECINTER S.A.	2245857

280	RENTSERVITOOL S.A. RENTA DE EQUIPOS Y SERVICIOS DE TECNOLOGIA	2480087
281	CARGRAPHICS S.A.	2401857
282	PRACTISIS S.A.	2229411
283	GLOBAL TELEMATIC SOLUTIONS GTSECUADOR S.A.	2272805
284	NEWAYS CIA. LTDA.	6006880
285	NAWESCORP CIA. LTDA.	2404702
286	SISERPROF SISTEMAS Y SERVICIOS PROFESIONALES CIA. LTDA.	2804472
287	INTEGRAL KNOWLEDGE INKNOW CIA. LTDA.	2241594
288	INTELISIS DEL ECUADOR ECUAINTELISIS S.A.	3520490
289	CENCOSSMART SOLUTIONS S.A.	2557913
290	ASISTENCIA TECNOLOGICA COOPERATIVA ASISTECOOPER S.A.	2443858
291	EQBONOBIT S.A.	2463012
292	BANTECINC S.A.	
293	NACCSYSTEMS DEL ECUADOR CIA. LTDA.	2243028
294	TICS ELITEL S.A.	2467491
295	COMPAÑIA CONSTRUCTORA Y DE REDES ELECTRICAS ISMAEL MEJIA R & M CIA. LTDA	096157886
296	COMINTECU COMUNICACIONES INTELIGENTES DEL ECUADOR CIA. LTDA.	3341472
297	ATIKASOFT CIA. LTDA.	2540077
298	FLIPBEAN S.A.	6002713
299	DO IT INFORMATION TECHNOLOGY AMERICA CIA. LTDA.	3332067
300	EBTECHSERVICE S.A.	2444701
301	DESEMCORP DESEMPEÑO CORPORATIVO S.A.	2434346
302	EGOVERMENT SOLUTIONS S.A. EGOVERSOLUT	2408732
303	CORPORACION WHITE LEAF SYSTEMS S.A.	2453230
304	CONSULTORES ALMEIDA LLERENA CIA. LTDA.	2463204
305	ADGESPROYECT CIA. LTDA.	2253580
306	QUITONET SOLUCIONES INFORMATICAS Y COMUNICACIONES CIA. LTDA.	2548943
307	MONEYLEVEL CIA. LTDA.	2243856
308	GARCIA OQUENDO CONSULTING CIA. LTDA.	2440858
309	MACCONTAINER S.A.	2867712
310	FRONTERA GLOBAL FRONGLOBAL CIA. LTDA.	2430653
311	SONDA DEL ECUADOR ECUASONDA S.A.	2468412
312	MODINTER S.A.	022237393
313	SOLUCIONES DE INFORMACION FIRAMI S.A.	2544692
314	COMPANIA CONSULTORA CONSULMATICA CIA LTDA	2252832
315	AUCONSIS CIA. LTDA.	2450885
316	INFORSYS CIA. LTDA.	022921891
317	LATINSYSTEM CIA. LTDA.	2412582
318	PRODUCTORA DE INFORMACION CIA. LTDA. PRODINFO	2522388
319	SMARTKARD S.A.	2041601
320	METAMORF S.A.	2236945
321	CREATECSA CREAR TECNOLOGIA S.A.	2222322
322	LLERENA & LLERENA SOFTWARE CIA. LTDA.	2494718
323	MULTI TECHNOLOGY INFORMATION CENTER MULTECIN S.A.	2955215
324	AVMEI ASESORIA, VENTA Y MANTENIMIENTO DE EQUIPOS INFORMATICOS CIA. LTDA.	2813214
325	SYGNUSEC S.A	2459491
326	GLOBAL COMUNICACIONES INTEGRALES GCINTEGRALES S.A	2455106
327	SOLUCIONES INTEGRALES GLOBALES, SOLINTEG S.A.	2562790
328	ECS ENERGY COMPUTER SYSTEMS CIA. LTDA.	2469740

329	V.W.O. ASESORIA INFORMATICA CIA. LTDA	22252427
330	POWERSOFT CIA. LTDA.	2591008
331	NEXT STEP C.A	2250017
332	INFORMATION TECHNOLOGY CONSULTING I.T. CONSULTING CIA. LTDA.	2455244
333	SISNAV CIA. LTDA.	2491902
334	PRISHARD PROFESIONALISMO CIA. LTDA.	2558864
335	TEMENOS ECUADOR S.A	2262550
336	ESPOIL DE ECUADOR C.A.	2243728
337	ROADTRACKING ECUADOR S.A.	2461444
338	TORRES QUEVEDO CIA. LTDA	2458711
339	SERVIBUSINESS S.A.	3341911
340	DIGITAL WARE LTDA.	6006956
341	DOCTORBYTE DEVELOPMENT CIA. LTDA.	2862713
342	PROGRAMACION, PASO Y SEGURIDAD, PROPASE C.A.	2454460
343	NETCONSUL CIA. LTDA.	2272912
344	SOLUCIONES DE NEGOCIOS SOFTNESA S. A.	2509464
345	MORRISTECH DEL ECUADOR S.A.	2482225
346	SOLUCIONES TECNOLOGICAS LEADSOLUTIONS CIA. LTDA.	2501789
347	SCIENCETECH S.A.	2433580
348	TECNOLOGIAS INFORMATICAS DEL ECUADOR VILSAMA CIA. LTDA.	2675954
349	FRAMEWORKS CIA. LTDA.	2254608
350	PIXELAR MULTIMEDIA CIA. LTDA.	2252440
351	ENCAJA TECHNOLOGIES ENCAJATECH CIA. LTDA.	
352	DESCASERV ECUADOR S.A.	2546440
353	SISTEMAS INFORMATICOS Y AGRICOLAS A LA MEDIDA SINAMED CIA. LTDA.	2456424
354	CELTELEFON S.A.	2223222
355	ATECH BUSINESS SOLUTIONS CIA. LTDA.	2473124
356	REALSEC S.A.	2266281
357	TELLINKSYS CIA. LTDA.	2501988
358	HOODGROUP ECUADOR CIA. LTDA.	2508676
359	NUEVAINTERNET CIA. LTDA.	2241599
360	LEVEL TECHNOLOGY SOLUCIONES EMPRESARIALES TECNOLOGICAS S.A.	2462364
361	LINKDESIGN CIA. LTDA.	022238752
362	SOLUCIONES INFORMATICAS EN SOFTWARE Y REDES ERASOFT CIA. LTDA.	2974401
363	DIVERBUSINESS CIA. LTDA	
364	INFORMATION TECHNOLOGIES ITWORKS CIA. LTDA.	2895031
365	QMF QUALITY MANAGEMENT FOCUS DEL ECUADOR S.A.	2646443
366	DAYRAMOR S.A.	2226491
367	OSHYN, INC.	2042134
368	DESARROLLO DE APLICACIONES EMPRESARIALES SAVIASOFT CIA. LTDA.	2340973

NEXO 2: ENCUESTA A LAS EMPRESAS DESARROLLADORAS DE SOFTWARE

ENCUESTA A LAS EMPRESAS DESARROLLADORAS DE SOFTWARE

Lea atentamente las instrucciones:

1. Este cuestionario contiene 60 preguntas. Las preguntas tienen como propósito realizar el análisis del medio de las empresas desarrolladoras de software existentes en la cuidad de Quito.
2. Para contestar marque con una X en la opción que este acorde a la realidad de su empresa.
3. Toda la información proporcionada por la empresa será utilizada únicamente con fines académicos.

Conteste las siguientes preguntas:

1. ¿Tiene definido un plan estratégico de TI y este se encuentra alineada con las necesidades del negocio?

   Si_____ Parcialmente_____ No_____

2. ¿Tiene definida su arquitectura de la información?

   Si_____ Parcialmente_____ No_____

3. ¿Cuenta con diccionario de datos empresarial?

   Si_____ Parcialmente_____ No_____

4. ¿El plan de la infraestructura tecnológica esta alineada con la arquitectura de la información?

   Si_____ Parcialmente_____ No_____

5. ¿Tiene definido un marco de trabajo de procesos para TI?

   Si_____ Parcialmente_____ No_____

6. ¿El presupuesto que se invierte para las operaciones de TI es el adecuado?

Si_____ Parcialmente_____ No_____

7. ¿Tiene implantado políticas de TI?

   Si_____ Parcialmente_____ No_____

   Si su respuesta fue SI, ¿con qué frecuencia son renovadas dichas políticas de TI?

   ____ Frecuentemente

   ____ A veces

   ____ Casi nunca

8. ¿El personal de TI es capacitado constantemente?

   Si_____ Parcialmente_____ No_____

9. ¿Están definidos los estándares y prácticas de calidad en la empresa?

   Si_____ Parcialmente_____ No_____

10. ¿Están identificados las amenazas y vulnerabilidades que afectan al normal desempeño de la empresa?

    Si_____ Parcialmente_____ No_____

    Si su respuesta fue SI, ¿cuáles son las amenazas y vulnerabilidades que causan mayor impacto en las operaciones de TI? Cite las más representativas

    _____

    _____

    _____

    _____

11. ¿Está usted preparado para enfrentar los riesgos que se presente en la empresa?

    Si_____ Parcialmente_____ No_____

12. ¿Los proyectos que se están ejecutando actualmente están dentro del plan Organizacional de la empresa?

    Si_____ Parcialmente_____ No_____

13. Previo a la compra o desarrollo de una solución automatizada, ¿se realiza un estudio de factibilidad?

    Si_____ Parcialmente_____ No_____

    Si su respuesta fue SI, ¿quién es el encargado de aprobar dicho estudio de factibilidad?

    _____

    _____

14. ¿Cuáles de los siguientes procesos utiliza para el desarrollo y mantenimiento del software de aplicación?

    ____ Diseño de alto nivel.
    ____ Diseño detallado.
    ____ Control y auditabilidad de las aplicaciones.
    ____ Control y auditabilidad de las aplicaciones.
    ____ Seguridad y disponibilidad de las aplicaciones.
    ____ Configuración e implantación de software aplicativo adquirido.
    ____ Actualizaciones importantes en sistemas existentes.
    ____ Desarrollo de software aplicativo.
    ____ Aseguramiento de la Calidad del Software.
    ____ Administración de los requerimientos de aplicaciones.
    ____ Mantenimiento de software aplicativo.
    ____ Otros

15. ¿Cuenta con las plataformas adecuadas para las aplicaciones de la empresa?

    Si_____ Parcialmente_____ No_____

16. ¿Qué actividades realiza para facilitar la operación y uso de los nuevos sistemas?

    ____ Desarrollar y hacer disponible la documentación de transferencia del conocimiento.

    ____ Participar y entrenar a usuarios y a la gerencia del negocio, personal de soporte y personal de operación.

    ____ Generar materiales de entrenamiento.

    ____ Otros

17. ¿Cuenta con todos los recursos de TI que necesita?

    Si_____ Parcialmente_____ No_____

18. ¿Quién es el responsable en evaluar, priorizar y autorizar los cambios dentro del ambiente de producción?

    ____ Propietario del proceso del negocio

    ____ Jefe de desarrollo

    ____ Director de administración de proyectos (PMO)

    ____ Jefe de operaciones

    ____ Otros

19. ¿Con que frecuencia se realizan cambios de emergencia en la infraestructura de TI, aplicaciones y soluciones técnicas?

    ____ Frecuentemente

    ____ A veces

    ____ Casi nunca

20. Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. ¿En la empresa se establecen metodologías de prueba para garantizar la aceptación del producto antes de ser liberado?

    Si_____ Parcialmente_____ No_____

21. ¿Se realizan planes de liberación de software (release)?

    Si_____ Parcialmente_____ No_____

22. ¿La gerencia es la encargada de realizar la evaluación formal y la aprobación de los resultados de prueba?

Si_____ Parcialmente_____ No_____

23. ¿Se ejecutan revisiones posteriores a la implantación?

Si_____ Parcialmente_____ No_____

24. ¿El nivel del servicio que se requiere esta acorde con los criterios de rendimiento del negocio?

Si_____ Parcialmente_____ No_____

25. ¿Tiene identificado y categorizado los servicios de su proveedor?

Si_____ Parcialmente_____ No_____

26. ¿Si su plan falla tiene algún plan para mitigar dicho riesgo?

Si_____ Parcialmente_____ No_____

27. ¿Están optimizados el desempeño de la infraestructura, los recursos y capacidades de TI en respuesta a las necesidades del negocio?

Si_____ Parcialmente_____ No_____

28. ¿Qué actividades se realizó para evaluar el desempeño del sistema?

____ Monitoreo del sistema.
____ Reporte del desempeño del sistema.
____ Modelado del sistema.
____ Pronóstico del sistema.
____ Otros

29. ¿La empresa cuenta con un plan de continuidad de TI?

Si_____ Parcialmente_____ No_____

Si su respuesta fue SI, ¿Están identificados los puntos más críticos en el plan de continuidad de TI?

Si_____ Parcialmente_____ No_____

30. ¿Qué operaciones o actividades se realiza con el plan de continuidad?

____ Mantenimiento del plan de continuidad de TI

____ Pruebas del plan de continuidad de TI

____ Entrenamiento del plan de continuidad de TI.

____ Distribución del plan de continuidad de TI

____ Otros

31. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad. ¿La empresa tiene una efectiva administracion de seguridad?

Si_____ Parcialmente_____ No_____

32. ¿El nivel de seguridad para salvaguardar la información contra el uso, revelación o modificación no autorizada, daño o pérdida es el adecuado?

Si_____ Parcialmente_____ No_____

33. ¿Qué operaciones o actividades se realiza para garantizar la seguridad de los sistemas?

____ Administración de la seguridad de TI

____ Plan de seguridad de TI

____ Administración de identidad

____ Administración de cuentas del usuario

____ Pruebas, vigilancia y monitoreo de la seguridad

____ Definición de incidente de seguridad

____ Protección de la tecnología de seguridad

____ Administración de llaves criptográficas

____ Prevención, detección y corrección de software malicioso

____ Seguridad de la red

____ Intercambio de datos sensitivos

____ Otros

34. ¿Los servicios de TI utilizan un sistema de contabilidad de costos para asegurar que los costos sean registrados, calculados y asignados al nivel requerido de detalle y a la oferta apropiada de servicio?

    Si_____ Parcialmente_____ No_____

35. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios, ¿La empresa cuenta con un plan de entrenamiento?

    Si_____ Parcialmente_____ No_____

36. ¿Cuántas sesiones de entrenamiento se realizan anualmente en la empresa?_____

37. Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y bien ejecutada, y de un proceso de administración de incidentes. ¿La empresa cuenta con una mesa de servicios y procesos para la administración de incidentes?

    Si_____ Parcialmente_____ No_____

38. ¿La empresa cuenta con un repositorio central que contenga toda la información referente a los elementos de configuración?

    Si_____ Parcialmente_____ No_____

39. ¿Los incidentes que suceden en la empresa están registrados y procesados en un sistema de administración de problemas?

    Si_____ Parcialmente_____ No_____

Si su respuesta fue SI, ¿Que actividades realiza para la administración de problemas?

____ Identificación y clasificación de problemas

____ Análisis de las causas desde su raíz

____ Resolución de problemas

____ Identificación de recomendaciones para la mejora

____ Mantenimiento de registros de problemas

____ Revisión del estatus de las acciones correctivas

____ Otros

40. ¿Optimiza el uso de la información y garantiza la disponibilidad de la misma cuando se requiera?

Si_____ Parcialmente_____ No_____

41. ¿Lleva inventario de medios de almacenamientos de datos en sitio y fuera del mismo?

Si_____ Parcialmente_____ No_____

42. ¿Minimiza el riesgo de una interrupción del servicio que presta?

Si_____ Parcialmente_____ No_____

43. ¿Implementan medidas físicas de seguridad con todos los elementos que forman parte de la empresa?

Si_____ Parcialmente_____ No_____

44. ¿Diseña e implementa medidas de protección contra factores ambientales?

Si_____ Parcialmente_____ No_____

45. ¿Mantiene la integridad de los datos y garantiza que la infraestructura de TI pueda resistir y recuperarse de errores y fallas?

Si_____ Parcialmente_____ No_____

46. ¿La empresa define y recolecciona datos de monitoreo del desempeño de TI?

Si_____ Parcialmente_____ No_____

47. ¿Compara periódicamente el desempeño de TI contra las metas de TI?

Si_____ Parcialmente_____ No_____

48. ¿Proporciona reportes administrativos del desempeño de TI a la alta dirección?

Si_____ Parcialmente_____ No_____

49. ¿Si monitorea el desempeño de TI, identifica e inicia medidas correctivas?

Si_____ Parcialmente_____ No_____

50. ¿Define un sistema de controles internos integrados al marco de trabajo de procesos de TI?

Si_____ Parcialmente_____ No_____

51. ¿Monitorea y reporta la efectividad de los controles internos sobre TI?

Si_____ Parcialmente_____ No_____

52. ¿Reporta las excepciones de control a la gerencia para tomar acciones?

Si_____ Parcialmente_____ No_____

53. ¿Identifica las leyes y regulaciones con impacto potencial sobre TI?

Si_____ Parcialmente_____ No_____

Si su respuesta fue SI, ¿Que actividades realiza para garantizar el cumplimiento regulatorio?

____ Identificar los requisitos legales y regulatorios con TI.

____ Entrenar al personal de TI sobre su responsabilidad de cumplimiento.

____ Evaluar el impacto de los requisitos regulatorios.

____ Monitorear y reportar el cumplimiento de los requerimietos regulatorios.

____ Otros

54. ¿Trabaja con el consejo directivo para definir y establecer un marco de trabajo para el gobierno de TI?

Si_____ Parcialmente_____ No_____

55. ¿Administra los programas de inversiones habilitados con TI, así como otros activos y servicios de TI?

Si_____ Parcialmente_____ No_____

56. ¿Trabaja en conjunto con el concejo directivo para definir el nivel de riesgo de TI aceptable por la empresa?

Si_____ Parcialmente_____ No_____

57. ¿Informa el desempeño relevante de los programas de TI al consejo directivo y a los ejecutivos de manera oportuna y precisa?

Si_____ Parcialmente_____ No_____

58. ¿Garantiza que la organización establezca y mantenga una función competente y que cuente con el personal adecuado y/o busque servicios de aseguramiento externo para proporcionar al concejo directivo?

Si_____ Parcialmente_____ No_____

ANEXO 3: COSO SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

COSO Sponsoring Organizations of the Treadway Commission

INTRODUCCION

El control interno, ha sufrido un cambio radical, cambio que si bien es cierto, ha permitido desde 1993 conceptualizar un nuevo estándar de control interno llamado C.O.S.O. (Commite of sponsoring Organizations of the Treadway Commission).

COMPONENTES DE CONTROL INTERNO

EL NUEVO ENFOQUE BASADO EN EL ESTÁNDAR INTERNACIONAL

Este enfoque involucra evaluar el funcionamiento del modelo de control interno corporativo C.O.S.O.; el que tiene los siguientes elementos constitutivos, que gráficamente se mostraron en el grafico anterior

I El entorno de control ;
II La medición de riesgos;
III El control de actividades;
IV El sistema de monitoreo;
V Los sistemas de comunicación;

VI Los sistemas de información;

Para el análisis de resultados se tomara como referencia el cuadro de interpretación conforme lo sugiere COSO Sponsoring Organizations of the Treadway Commission para la aplicación de los cuestionarios de control interno.

CALIF. %		GC	NR
15%	33%	B	A
34%	70%	M	M
71%	99%	A	B

M	MODERADO
B	BAJO
A	ALTO
GC	GRADO DE CONFIANZA

Tabla 59: Cuadro de Interpretación[1]

Publicado en 1992 hace recomendaciones a los contables de gestión como evaluar, informar e implementar sistemas de control teniendo como objetivo de control la efectividad y eficiencia de las operaciones, la información financiera y el cumplimiento de las regulaciones que explica en los componentes del ambiente de control, valoración de riesgos, actividades de control, información y comunicación, y el monitoreo.

[1] Cuadro de Interpretación, utilizado en la Dirección de Auditoría Interna de la Escuela Politécnica Nacional.

ANEXO 4: FORMULACIÒN DEL PROCESO (CUESTIONARIO)

FORMULACIÒN DEL PROCESO (CUESTIONARIO)

PLANIFICAR Y ORGANIZAR

PO1: Definir un plan estratégico para TI

FACTORES A CONSIDERAR PARA DEFINIR UN PLAN ESTRATÉGICO DE TI **Se debe verificar si:**	SI	PARCIALMENTE	NO
Tiene definido un plan estratégico de TI y este se encuentra alineado con las necesidades del negocio.			
Realiza la evaluación del desempeño de los planes existentes y de los sistemas de información.			
Traduce el plan estratégico de TI a planes tácticos.			
Analiza portafolios de programas y se administra portafolios de servicios y proyectos.			

PO2: Definir la arquitectura de la información

FACTORES A CONSIDERAR PARA DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN **Se debe verificar si:**	SI	PARCIALMENTE	NO
Tiene definida la arquitectura de la información.			
Cuenta con un diccionario de datos empresarial.			

PO5: Administrar la inversión en TI.

FACTORES A CONSIDERAR PARA ADMINISTRAR LA INVERSIÓN EN TI. **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece un marco de trabajo financiero para TI que impulse el presupuesto y el análisis de rentabilidad, con base en los portafolios de inversión, servicios y activos.			
Se implanta un proceso de toma de decisiones para dar prioridades a la asignación de recursos de TI.			
Establece y mantiene un proceso presupuestal de TI.			
Implanta un proceso de administración de costos que compare los costos reales con los presupuestados.			
Implanta un proceso de monitoreo de beneficios			

PO6: Comunicar las aspiraciones y la dirección de la gerencia.

FACTORES A CONSIDERAR PARA COMUNICAR LAS ASPIRACIONES Y LA DIRECCIÓN DE LA GERENCIA **Se debe verificar si:**	SI	PARCIALMENTE	NO
Define los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa.			
Elabora y da mantenimiento a un marco de trabajo enfocado en los riesgos y control interno, para entregar valor mientras al mismo tiempo se protegen los recursos y sistemas de TI.			
Elabora y da mantenimiento a un conjunto de políticas que apoyen la estrategia de TI.			
Implantan y comunican las políticas de TI al personal que le compete.			
Asegura que la conciencia y el entendimiento de los objetivos de la dirección del negocio y de TI se comunican a toda la organización.			

PO7: Administrar los recursos humanos de TI

FACTORES A CONSIDERAR PARA ADMINISTRAR LOS RECURSOS HUMANOS DE TI **Se debe verificar si:**	SI	PARCIALMENTE	NO
Asegura que el reclutamiento del personal de TI se lleve a cabo de acuerdo a políticas y procedimientos generales de personal de la organización.			
Verifica periódicamente que el personal este capacitado.			
Define, monitorea y supervisa los marcos de trabajo para los roles, responsabilidades y compensación del personal en base a políticas administrativas.			
Capacita constantemente al personal de TI.			
Minimiza el grado de dependencia del personal indispensable.			
Minimiza el riesgo del cambio de puesto o terminación del trabajo del personal.			

PO8: Administrar la calidad

FACTORES A CONSIDERAR PARA ADMINISTRAR LA	SI	PARCIALMENTE	NO

CALIDAD **Se debe verificar si:**			
Monitorea y mide la efectividad y aceptación del QMS y lo mejora cuando sea necesario.			
Identifica y mantiene estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del QMS.			
Adopta y mantiene estándares para todo el desarrollo y adquisición que sigue el ciclo de vida hasta el último entregable.			
Garantiza que la administración de calidad se enfoquen los clientes, determine sus requerimientos y los alinee con los estándares y prácticas de TI.			
Elabora y comunica un plan global de calidad que promueva la mejora continua, de forma periódica.			
Define, planea e implementa mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que este proporciona.			

PO9: Evaluar y administrar los riesgos de TI.

FACTORES A CONSIDERAR PARA EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI. **Se debe verificar si:**	SI	PARCIALMENTE	NO
Integra el gobierno, la administración de riesgos y el marco de control de TI., al marco de trabajo de administración de riesgos de la organización.			
Establece el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados.			
Identifica las amenazas y vulnerabilidades que afectan al normal desempeño de la empresa.			
Evalúa de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos.			
Elabora y mantiene respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continua.			
Asigna prioridades y planea las actividades de control a todos los			

niveles para implantar las respuestas a los riesgos, identificadas como necesarios, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución.			

PO10: Administrar Proyectos

FACTORES A CONSIDERAR PARA ADMINISTRAR PROYECTOS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Mantiene el programa de los proyectos, relacionados con el portafolio de los programas de inversión en TI.			
Establece y mantiene un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas.			
Establece un enfoque de administración de proyectos que corresponda al tamaño complejidad y requerimientos regulatorios de cada proyecto.			
Asegura que todos los proyectos de TI cuenten con patrocinadores con la suficiente autoridad para apropiarse de la ejecución del proyecto dentro del programa estratégico global.			
Obtiene el compromiso y participación de los interesados afectados en la definición y ejecución del proyecto dentro del contexto del programa global de inversión en TI.			
Define y documenta la naturaleza y alcance del proyecto para conformar y desarrollar, entre los interesados, un entendimiento común del alcance del proyecto y su relación con otros proyectos dentro del programa global de inversiones en TI.			
Asegura que el arranque de las etapas importantes del proyecto se aprueben de manera formal y se comunique a todos los interesados.			
Establece un plan integrado para el proyecto, aprobado y formal para guiar la ejecución y control del proyecto a lo largo de la vida de este.			
Entiende y documenta dentro de un mismo programa las actividades e interdependencias de múltiples proyectos.			

Define las responsabilidades, relaciones, autoridades y criterios de desempeño de los miembros del equipo del proyecto y especifica las bases para adquirir y asignar a los miembros competentes del equipo y/o los contratistas al proyecto.			
Eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, análisis, respuesta, monitoreo y control de las áreas o eventos que tenga el potencial de ocasionar cambios no deseados.			
Prepara un plan de administración de la calidad que describa el sistema de calidad del proyecto y como será implantado.			
Revisa y acuerda el plan de calidad de proyecto con todas las partes interesadas para luego ser incorporado en el plan integrado del proyecto.			
Establece un sistema de control de cambios para cada proyecto, de tal modo que todos los cambios a la línea base del proyecto se revisen, aprueben e incorporen de manera apropiada al plan integrado del proyecto, de acuerdo al marco de trabajo del gobierno del programa y del proyecto.			
Identifica las tareas de aseguramiento requeridas para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado.			
Mide el desempeño del proyecto contra los criterios claves del proyecto y recomienda, implanta y monitorea las medidas correctivas según sea requerido, de acuerdo con el marco de trabajo de gobierno del programa y del proyecto.			
Solicita que al finalizar cada proyecto, los interesados del proyecto se cercioren de que el proyecto haya cubierto los resultados y beneficios esperados.			

ADQUIRIR E IMPLEMENTAR

AI2: Adquirir y mantener software aplicativo.

FACTORES A CONSIDERAR PARA ADQUIRIR Y MANTENER SOFTWARE APLICATIVO. **Se debe verificar si:**	SI	PARCIALMENTE	NO
Traduce los requerimientos del negocio a una especificación de			

diseño de alto nivel para desarrollo de software, y aprueba las especificaciones de diseño para garantizar que el diseño de alto nivel responde a los requerimientos.			
Prepara el diseño detallado y los requerimientos técnicos del software de aplicación.			
Define el criterio de aceptación de los requerimientos y aprobar los requerimientos para garantizar que corresponden al diseño de alto nivel.			
Realiza una reevaluación para cuando se presenten discrepancias técnicas o lógicas significativas durante el desarrollo o mantenimiento.			
Asegura que los controles del negocio se traduzcan correctamente en controles de aplicación de manera que el procesamiento sea exacto, completo, oportuno, aprobado y auditable.			
Aborda la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados, de acuerdo con la clasificación de datos, la arquitectura de seguridad en la información de la organización y el perfil de riesgo.			
Personaliza e implanta la funcionalidad automatizada adquirida con el uso de procedimientos de configuración, aceptación y prueba.			
Sigue un proceso de desarrollo similar al de desarrollo de sistemas nuevos en el caso que se presenten modificaciones importantes en los sistemas existentes, que resulten en un cambio significativo de los diseños y/o funcionalidad actuales.			
Garantiza que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación y los requerimientos de calidad.			
Aprueba y autoriza cada etapa clave del proceso de desarrollo de software aplicativo, dando seguimiento a la terminación exitosa de revisiones de funcionalidad, desempeño y calidad.			
Garantiza que se identifican y consideran todos los aspectos legales y contractuales para el software aplicativo que desarrollan terceros.			
Desarrolla, implanta los recursos y ejecuta un plan de			

aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización.			
Garantiza que durante el diseño, desarrollo e implantación, se da seguimiento al estatus de los requerimientos particulares (incluyendo todos los requerimientos rechazados), y que las modificaciones a los requerimientos se aprueban a través de un proceso establecido de administración de cambios.			
Desarrolla una estrategia y un plan para el mantenimiento y liberación de aplicaciones de software.			

AI3: Adquirir y mantener infraestructura tecnológica.

FACTORES A CONSIDERAR PARA ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA. **Se debe verificar si:**	SI	PARCIALMENTE	NO
Genera un plan para adquirir, implantar y mantener a infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización.			
Implanta medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del HW y SW de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.			
Establece ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura en las primeras fases del proceso de adquisición y desarrollo.			

AI4: Facilitar la operación y el uso

FACTORES A CONSIDERAR PARA FACILITAR LA OPEERACIÓN Y EL USO **Se debe verificar si:**	SI	PARCIALMENTE	NO
Desarrolla un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos para llevar acabo las operaciones de TI.			

Transfiere el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos, y ejercer la responsabilidad por la entrega y calidad del servicio, del control interno y de los procesos administrativos de la aplicación.			
Transfiere conocimientos y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de aplicación como apoyo, a los procesos del negocio.			
Transfiere conocimientos y habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos.			

AI5: Adquirir recursos de TI.

FACTORES A CONSIDERAR PARA ADQUIRIR RECURSOS DE TI **Se debe verificar si:**	SI	PARCIALMENTE	NO
Desarrolla y sigue un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición, para garantizar que la adquisición de infraestructura, instalaciones, hardware, software y servicios relacionados con TI, satisfagan los requerimientos del negocio.			
Formula un procedimiento para establecer, modificar y concluir contratos que apliquen a todos los proveedores.			
Selecciona proveedores mediante una práctica justa y formal para garantizar la escogencia del mejor con base en los requerimientos que se han desarrollado con información de proveedores potenciales y acordados entre el cliente y el(los) proveedor(es).			
Incluye y refuerza los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de software involucrados en el suministro y uso continuo de software.			
Incluye y hace cumplir los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de recursos de desarrollo.			

Incluye y hace cumplir los derechos y obligaciones de todas las partes en los términos contractuales, que comprendan los criterios de aceptación, para la adquisición de infraestructura, instalaciones y servicios relacionados.			

AI6: Administrar cambios

FACTORES A CONSIDERAR PARA ADMINISTRAR CAMBIOS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.			
Garantiza que todas las solicitudes de cambio se evalúan de una manera estructurada en cuanto a impactos en el sistema operacional y su funcionalidad.			
Establece un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido.			
Establece un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales.			
Actualiza el sistema asociado y la documentación de usuario y procedimientos siempre que se implantan cambios al sistema.			
Establece un proceso de revisión para garantizar la implantación completa de los cambios.			

AI7: Instalar y acreditar soluciones y cambios.

FACTORES A CONSIDERAR PARA INSTALAR Y ACREDITAR SOLUCIONES Y CAMBIOS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Entrena al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan			

definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de desarrollo, implantación o modificación de sistemas de información.			
Establece un plan de pruebas y obtener la aprobación de las partes relevantes.			
Establece un plan de implantación y obtener la aprobación de las partes relevantes.			
Establece un ambiente de prueba que refleje el ambiente futuro de operaciones para permitir pruebas acertadas.			
Garantiza que los componentes sean convertidos del viejo al nuevo sistema de acuerdo con un plan preestablecido.			
Garantiza que se prueban los cambios de acuerdo con el plan de aceptación definido y en base en una evaluación de impacto y recursos.			
Garantiza que los procedimientos proporcionan, como parte de la aceptación final o prueba de aseguramientos de la calidad de los sistemas de información nuevos o modificados, una evaluación formal y la aprobación de los resultados de prueba por parte de la gerencia de los departamentos afectados del usuario y la función de TI.			
Implanta procedimientos formales para controlar la transferencia del sistema desde el ambiente de desarrollo al de pruebas, de acuerdo con el plan de implantación.			
Garantiza que la liberación del software se regula con procedimientos formales que aseguren la autorización, acondicionamiento, pruebas de regresión, distribución, transferencia de control, rastreo de estatus, procedimientos de respaldo y notificación de usuario.			
Establece procedimientos de control para asegurar la distribución oportuna y correcta, y la actualización de los componentes aprobados de la configuración.			
Automatiza el sistema utilizado para monitorear cambios a sistemas aplicativos para soportar el registro y rastreo de cambios hechos en aplicaciones, procedimientos, procesos, sistemas y parámetros de servicio, y a las plataformas subyacentes.			

Establece procedimientos de acuerdo con los estándares de desarrollo y de cambios de la empresa, que requieren una revisión posterior a la implantación del sistema de información en operación para evaluar y reportar si el cambio satisfizo los requerimientos del cliente y entregó los beneficios visualizados, de la forma más rentable.			

ENTREGAR Y DAR SOPORTE

DS2: Administrar servicios de terceros.

FACTORES A CONSIDERAR PARA ADMINISTRAR SERVICIOS DE TERCEROS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad.			
Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener una efectiva entrega de servicios de forma segura y eficiente sobre una base de continuidad.			
Asegurar que los contratos están de acuerdo con los estándares universales del negocio de conformidad con los requerimientos legales y regulatorios.			
Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con los requerimientos del negocio actuales y que se apega de manera continua a los acuerdos del contrato y a los convenios de niveles de servicio, y que el desempeño es competitivo respecto a los proveedores alternativos y a las condiciones del mercado.			

DS3: Administrar desempeño y capacidad.

FACTORES A CONSIDERAR PARA EVALUAR Y FACTORES A CONSIDERAR PARA ADMINISTRAR DESEMPEÑO Y CAPACIDAD **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, con costos			

justificables, para procesar las cargas de trabajo acordadas tal como se determina en los SLAs.			
Revisa la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados.			
Lleva a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño.			
Brinda la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI.			
Monitorea continuamente el desempeño y la capacidad de los recursos de TI.			

DS4: Garantizar la continuidad del servicio.

FACTORES A CONSIDERAR PARA GARANTIZAR LA CONTINUIDAD DEL SERVICIO. **Se debe verificar si:**	SI	PARCIALMENTE	NO
Desarrolla un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización.			
Desarrolla planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio.			
Centra la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.			
Exhorta a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio.			
Prueba el plan de continuidad de TI de forma regular para asegurar			

que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable.			
Asegura de que todos las partes involucradas reciban sesiones de capacitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.			
Determina que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera.			
Planea las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios.			
Almacena fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio.			

DS5: Garantizar la seguridad de los sistemas

FACTORES A CONSIDERAR PARA GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Administra la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.			
Traslada los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI.			
Identifica de manera única a todos los usuarios y su actividad en sistemas de TI.			
Garantiza que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario.			
Garantiza que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.			

Garantiza que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes.			
Garantiza que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria.			
Determina que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.			
Garantiza que se cuente con medidas de prevención, detección y corrección a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso			
Garantiza que se utilizan técnicas de seguridad y procedimientos de administración asociados para autorizar acceso y controlar los flujos de información desde y hacia las redes.			
Garantiza que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.			

DS6: Identificar y asignar costos

FACTORES A CONSIDERAR PARA IDENTIFICAR Y ASIGNAR COSTOS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Identifica todos los costos de TI y equipararlos a los servicios de TI para soportar un modelo de costos transparente.			
Registra y asigna los costos actuales de acuerdo con el modelo de costos definido.			
Define un modelo de costos que incluya costos directos, indirectos y fijos de los servicios, y que ayude al cálculo de tarifas de			

reintegros de cobro por servicio en base a la definición del servicio.			
Revisa y compara de forma regular lo apropiado del modelo de costos/recargos para mantener su relevancia para el negocio en evolución y para las actividades de TI.			

DS7: Educar y entrenar a los usuarios

FACTORES A CONSIDERAR PARA EDUCAR Y ENTRENAR A LOS USUARIOS **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece y actualiza de forma regular un programa de entrenamiento para cada grupo objetivo de empleados,			

DS8: Administrar la mesa de servicio y los incidentes

FACTORES A CONSIDERAR PARA ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información.			
Establece una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información.			
Establece procedimientos de mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente de acuerdo con los límites acordados en el SLA y, si es adecuado, brindar soluciones alternas.			
Garantiza que la asignación de incidentes y el monitoreo del ciclo de vida permanecen en la mesa de servicios, independientemente de qué grupo de TI esté trabajando en las actividades de resolución.			
Establece procedimientos para el monitoreo puntual de la			

resolución de consultas de los clientes.			
Emite reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.			

DS9: Administrar la configuración

FACTORES A CONSIDERAR PARA ADMINISTRACIÓN DE LA CONFIGURACIÓN **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece un repositorio central que contenga toda la información referente a los elementos de configuración.			
Revisa y verifica de manera regular, utilizando cuando sea necesario herramientas apropiadas, el estatus de los elementos de configuración para confirmar la integridad de la configuración de datos actual e histórica y para comparar con la situación actual.			

DS10: Administración de problemas

FACTORES A CONSIDERAR PARA ADMINISTRACIÓN DE PROBLEMAS **Se debe verificar si**	SI	PARCIALMENTE	NO
Implementa procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes			
Mantiene pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados.			
Identifica e inicia soluciones sostenibles indicando la causa raíz, incrementando las solicitudes de cambio por medio del proceso de administración de cambios establecido.			
Dispone de un procedimiento para cerrar registros de problemas ya sea después de confirmar la eliminación exitosa del error conocido o después de acordar con el negocio cómo manejar el problema de manera alternativa.			
Garantiza una adecuada administración de problemas e incidentes,			

integrar los procesos relacionados de administración de cambios, configuración y problemas.			

DS11: Administración de la Información

FACTORES A CONSIDERAR PARA ADMINISTRACIÓN DE LA INFORMACIÓN **Se debe verificar si:**	SI	PARCIALMENTE	NO
Establece mecanismos para garantizar que el negocio reciba los documentos originales que espera, que se procese toda la información recibida por parte del negocio, que se preparen y entreguen todos los reportes de salida que requiere el negocio y que las necesidades de reinicio y reproceso estén soportadas.			
Define e implementa procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables.			
Define e implementa procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y su uso.			
Define e implementa procedimientos para prevenir el acceso a datos sensitivos y al software desde equipos o medios una vez que son eliminados o transferidos para otro uso.			
Define e implementa procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad.			
Establece mecanismos para identificar y aplicar requerimientos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos.			

DS12: Administración del ambiente físico.

FACTORES A CONSIDERAR PARA ADMINISTRACIÓN DEL AMBIENTE FÍSICO **Se debe verificar si::**	SI	PARCIALMENTE	NO
Define e implementa medidas de seguridad físicas alineadas con los requerimientos del negocio.			
Diseña e implementa medidas de protección contra factores			

ambientales.			

DS13: Administración de Operaciones

FACTORES A CONSIDERAR PARA ADMINISTRACIÓN DE OPERACIONES **Se debe verificar si:**	SI	PARCIALMENTE	NO
Define, implementa y mantiene procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos.			
Organiza la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el rendimiento y la utilización para cumplir con los requerimientos del negocio.			
Garantiza que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones.			
Establece resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos tales como formas, instrumentos negociables, impresoras de uso especial o dispositivos de seguridad.			
Define e implementa procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.			

MONITOREAR Y EVALUAR

ME1: Monitorear y evaluar el desempeño de TI.

FACTORES A CONSIDERAR PARA MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI **Se debe verificar si::**	SI	PARCIALMENTE	NO
Garantiza que la gerencia establezca un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para monitorear la contribución de TI a los resultados de los procesos de administración de			

programas y de administración del portafolio empresarial y aquellos procesos que son específicos para la entrega de la capacidad y los servicios de TI.			
Garantiza que la gerencia de TI, trabajando en conjunto con el negocio, defina un conjunto balanceado de objetivos, mediciones, metas y comparaciones de desempeño y que estas se encuentren acordadas formalmente con el negocio y otros interesados relevantes.			
Garantiza que el proceso de monitoreo implante un método, que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa.			
Compara de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes.			
Proporciona reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño.			
Identifica e inicia medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes.			

ME2: Monitorear y evaluar el control interno.

FACTORES A CONSIDERAR PARA FACTORES A CONSIDERAR PARA MONITOREAR Y EVALUAR EL CONTROL INTERNO **Se debe verificar:**	SI	PARCIALMENTE	NO
Monitorea de forma continua el ambiente de control y el marco de control de TI.			
Monitorea y reporta la efectividad de los controles internos sobre TI por medio de revisiones de auditoría.			
Registra la información referente a todas las excepciones de control y garantizar que esto conduzca al análisis de las causas subyacentes y a la toma de acciones correctivas.			

Evalúa la completitud y efectividad de los controles internos de la administración de los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación.			
Obtiene, según sea necesario, aseguramiento adicional de la completitud y efectividad de los controles internos por medio de revisiones de terceros.			
Confirma que los proveedores externos de servicios cumplan con los requerimientos legales y regulatorios y con las obligaciones contractuales.			
Identifica e inicia medidas correctivas basadas en las evaluaciones y en los reportes de control.			

ME3: Garantizar el cumplimiento regulatorio.

FACTORES A CONSIDERAR PARA GARANTIZAR EL CUMPLIMIENTO REGULATORIO. **Se debe verificar si:**	SI	PARCIALMENTE	NO
Define e implanta un proceso para garantizar la identificación oportuna de requerimientos locales e internacionales legales, contractuales, de políticas y regulatorios, relacionados con la información, con la prestación de servicios de información incluyendo servicios de terceros y con la función, procesos e infraestructura de TI.			
Revisa y optimiza las políticas, estándares y procedimientos de TI para garantizar que los requisitos legales y regulatorios se cubran de forma eficiente.			
Evalúa de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requerimientos legales y regulatorios, con base en la supervisión del gobierno de la gerencia de TI y del negocio y la operación de los controles internos.			
Define e implanta procedimientos para obtener y reportar un aseguramiento del cumplimiento y, donde sea necesario, que el propietario del proceso haya tomado las medidas correctivas oportunas para resolver cualquier brecha de cumplimiento.			
Integra los reportes de TI sobre cumplimiento regulatorio con las			

salidas similares provenientes de otras funciones del negocio.			

ME4: Proporcionar Gobierno de TI.

FACTORES A CONSIDERAR PARA PROPORCIONAR GOBIERNO DE TI. **Se debe verificar si:**	SI	PARCIALMENTE	NO
Trabaja con el consejo directivo para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles y responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI de la empresa ofrezcan y estén alineados con las estrategias y objetivos empresariales.			
Facilita el entendimiento del consejo directivo y de los ejecutivos sobre temas estratégicos de TI tales como el rol de TI, características propias y capacidades de la tecnología.			
Garantiza que existe un entendimiento compartido entre el negocio y la función de TI sobre la contribución potencial de TI a la estrategia del negocio.			
Trabaja con el consejo directivo para definir e implantar organismos de gobierno, tales como un comité estratégico de TI, para brindar una orientación estratégica a la gerencia respecto a TI.			
Facilita la alineación de TI con el negocio en lo referente a estrategia y operaciones, fomentando la co-responsabilidad entre el negocio y TI en la toma de decisiones estratégicas y en la obtención de los beneficios provenientes de las inversiones habilitadas con TI.			
Administra los programas de inversión habilitados con TI, así como otros activos y servicios de TI, para asegurar que ofrezcan el mayor valor posible para apoyar la estrategia y los objetivos empresariales.			
Implanta un enfoque disciplinado hacia la administración por portafolio, programa y proyecto, enfatizando que el negocio asume la propiedad de todas las inversiones habilitadas con TI y que TI garantiza la optimización de los costos por la prestación de los servicios y capacidades de TI.			

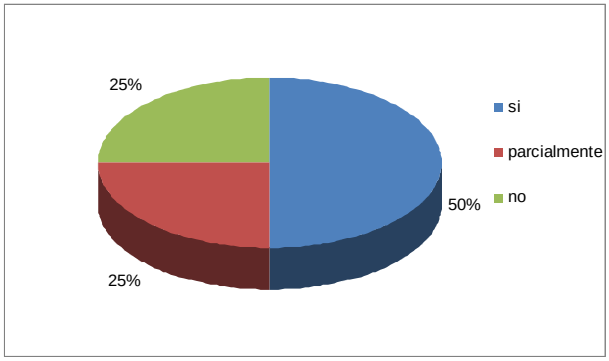
Asegura que las inversiones en tecnología estén estandarizadas a mayor grado posible para evitar el aumento en costo y complejidad de una proliferación de soluciones técnicas.			
Optimiza la inversión, uso y asignación de los activos de TI por medio de evaluaciones periódicas, garantizando que TI cuente con recursos suficientes, competentes y capaces para ejecutar los objetivos estratégicos actuales y futuros y seguir el ritmo de los requerimientos del negocio.			
Trabaja en conjunto con el consejo directivo para definir el nivel de riesgo de TI aceptable por la empresa.			
Comunica este nivel de riesgo hacia la organización y acordar el plan de administración de riesgos de TI.			
Integra las responsabilidades de administración de riesgos en la organización, asegurando que tanto el negocio como TI evalúen y reporten periódicamente los riesgos asociados con TI y su impacto en el negocio.			
Garantiza que la gerencia de TI haga seguimiento a la exposición a los riesgos, poniendo especial atención en las fallas y debilidades de control interno y de supervisión, así como su impacto actual y potencial en el negocio.			
Informa el desempeño relevante del portafolio de los programas de TI al consejo directivo y a los ejecutivos de manera oportuna y precisa.			
Garantiza que la organización establezca y mantenga una función competente y que cuente con el personal adecuado y/o busque servicios de aseguramiento externo para proporcionar al consejo directivo.			

ANEXO 5: RESULTADOS DE LA APLICACIÓN DEL PROCESO

RESULTADOS DE LA APLICACIÓN DEL PROCESO PLANIFICAR Y ORGANIZAR

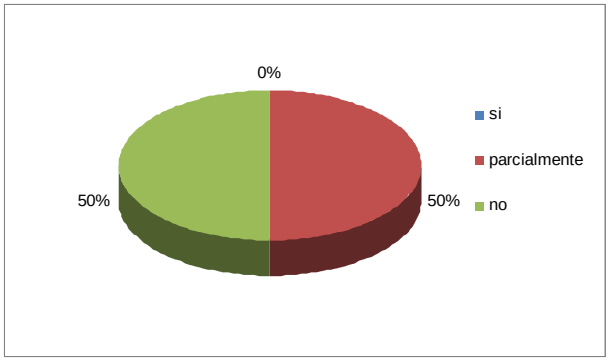
PO1: Definir un plan estratégico para TI

SI	PARCIALMENTE	NO
2	1	1



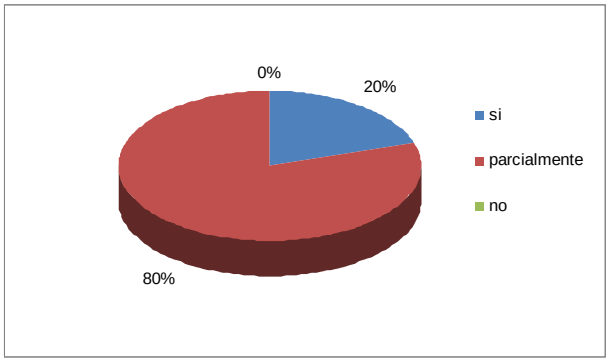
PO2: Definir la arquitectura de la información

SI	PARCIALMENTE	NO
0	1	1



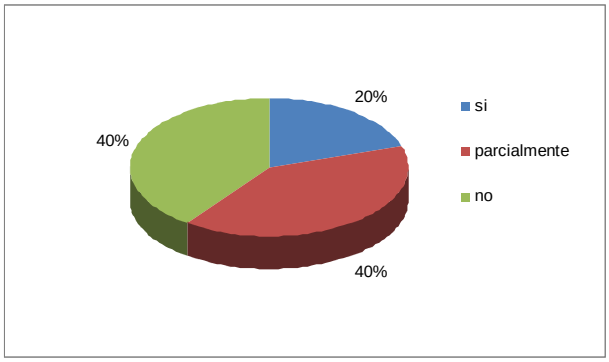
PO5: Administrar la inversión en TI.

SI	PARCIALMENTE	NO
1	4	0



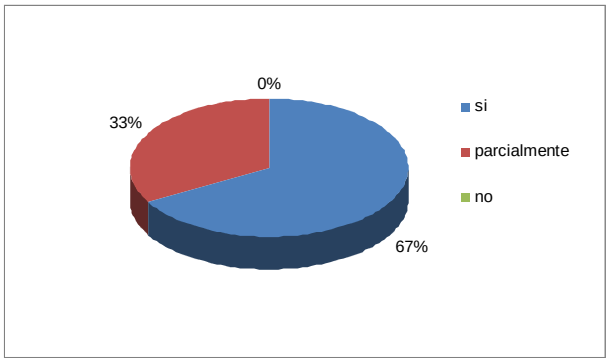
PO6: Comunicar las aspiraciones y la dirección de la gerencia.

SI	PARCIALMENTE	NO
1	2	2



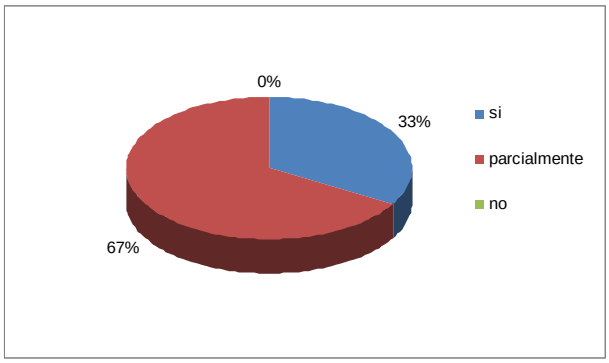
PO7: Administrar los recursos humanos de TI

SI	PARCIALMENTE	NO
4	2	0



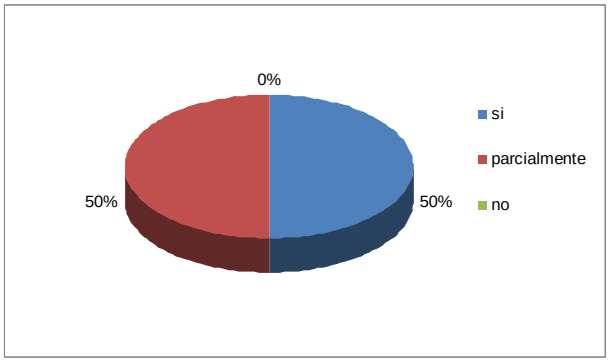
PO8: Administrar la calidad

SI	PARCIALMENTE	NO
2	4	0



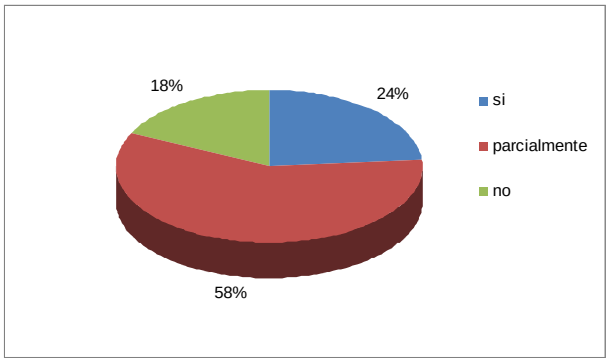
PO9: Evaluar y administrar los riesgos de TI.

SI	PARCIALMENTE	NO
3	3	0



PO10: Administrar Proyectos

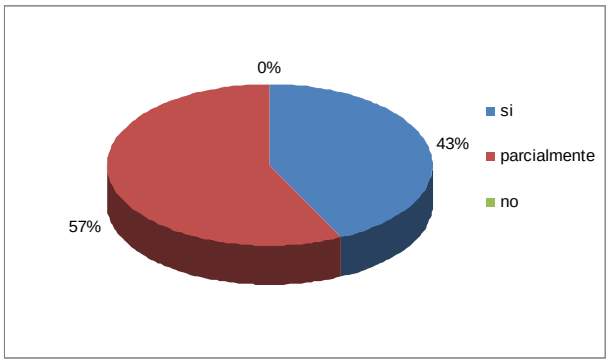
SI	PARCIALMENTE	NO
4	10	3



ADQUIRIR E IMPLEMENTAR

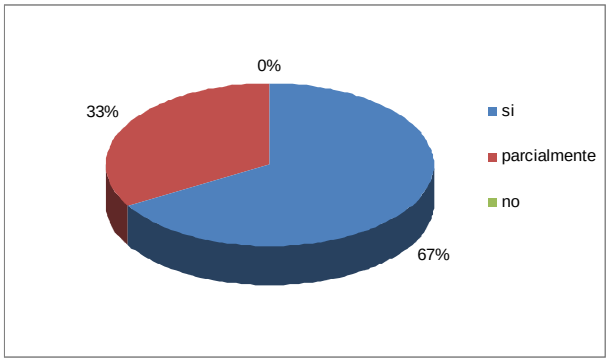
AI2: Adquirir y mantener software aplicativo.

SI	PARCIALMENTE	NO
6	8	0



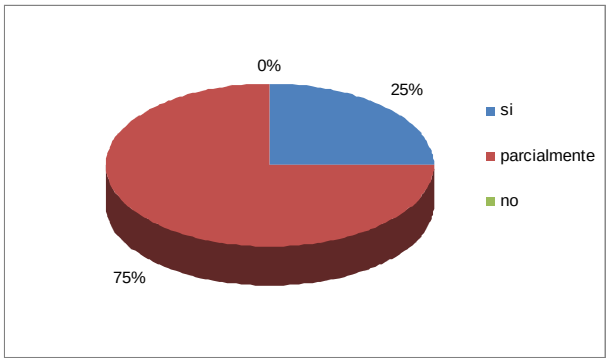
AI3: Adquirir y mantener infraestructura tecnológica.

SI	PARCIALMENTE	NO
2	1	0



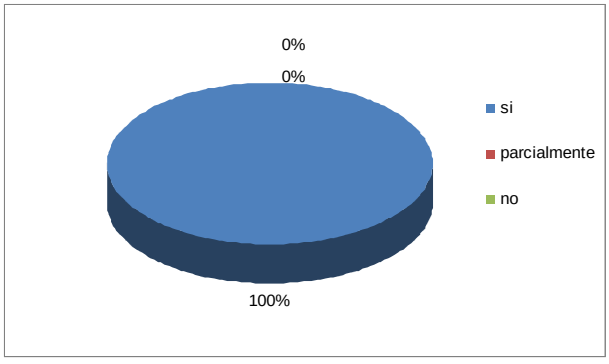
AI4: Facilitar la operación y el uso

SI	PARCIALMENTE	NO
1	3	0



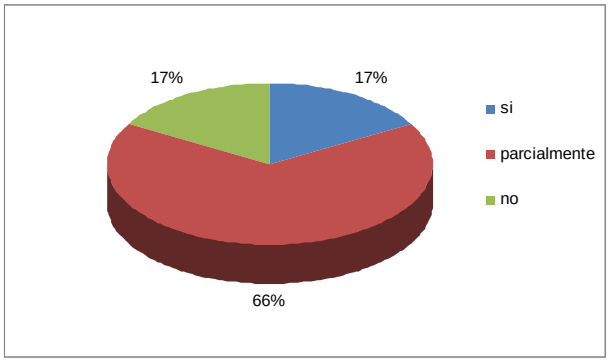
AI5: Adquirir recursos de TI.

SI	PARCIALMENTE	NO
6	0	0



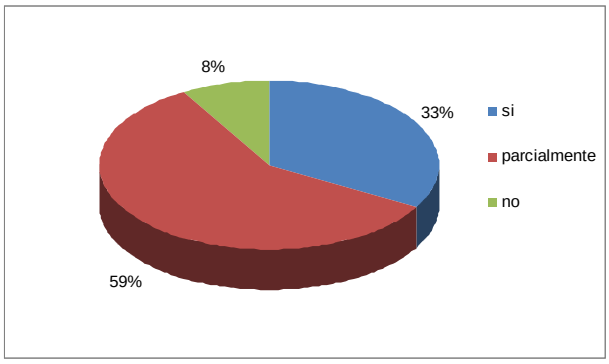
AI6: Administrar cambios

SI	PARCIALMENTE	NO
1	4	1



AI7: Instalar y acreditar soluciones y cambios.

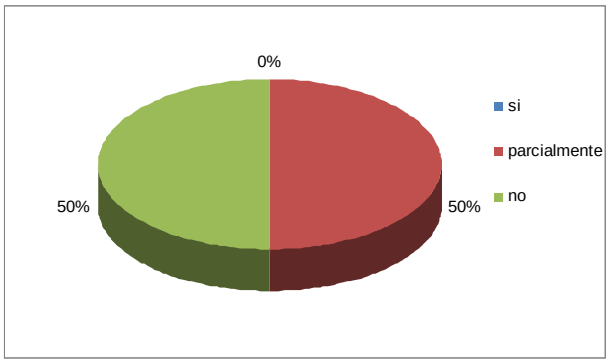
SI	PARCIALMENTE	NO
4	7	1



ENTREGAR Y DAR SOPORTE

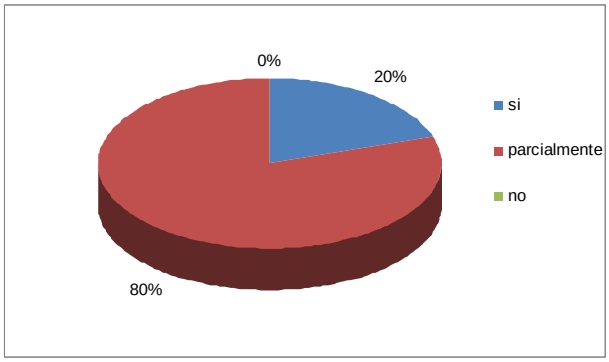
DS2: Administrar servicios de terceros.

SI	PARCIALMENTE	NO
0	2	2



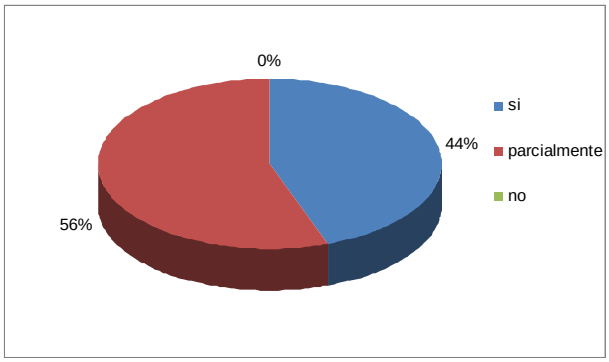
DS3: Administrar desempeño y capacidad.

SI	PARCIALMENTE	NO
1	4	0



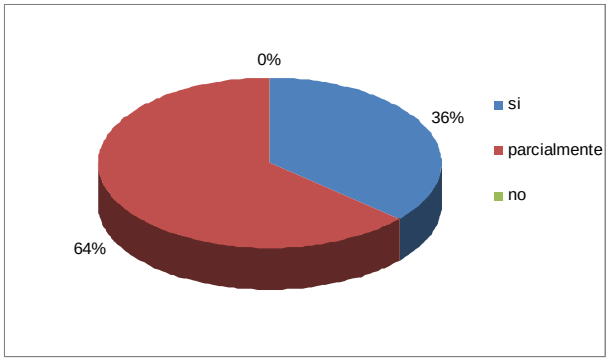
DS4: Garantizar la continuidad del servicio.

SI	PARCIALMENTE	NO
4	5	0



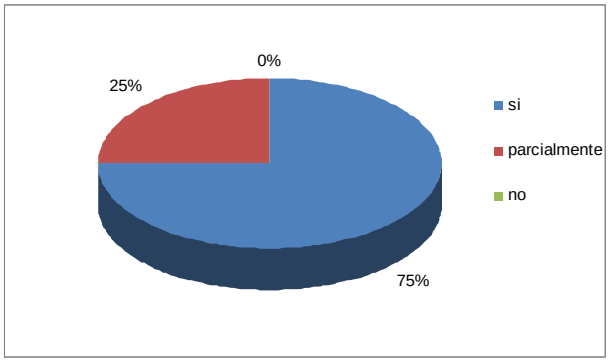
DS5: Garantizar la seguridad de los sistemas

SI	PARCIALMENTE	NO
4	7	0



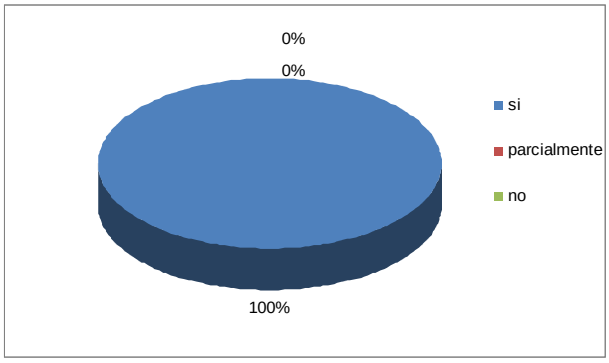
DS6: Identificar y asignar costos

SI	PARCIALMENTE	NO
3	1	0



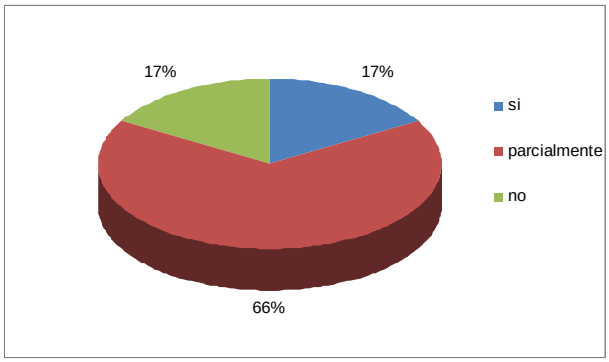
DS7: Educar y entrenar a los usuarios

SI	PARCIALMENTE	NO
1	0	0



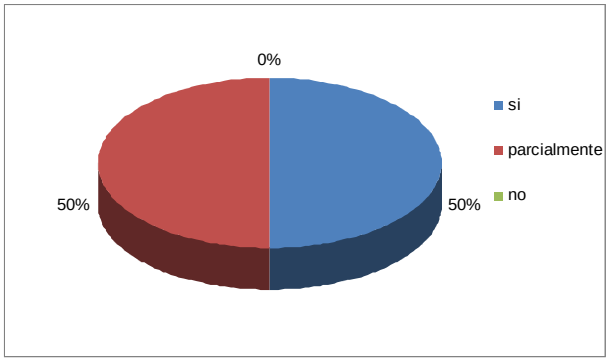
DS8: Administrar la mesa de servicio y los incidentes

SI	PARCIALMENTE	NO
1	4	1



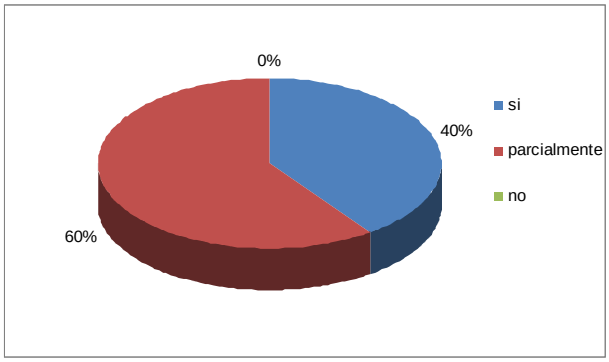
DS9: Administrar la configuración

SI	PARCIALMENTE	NO
1	1	0



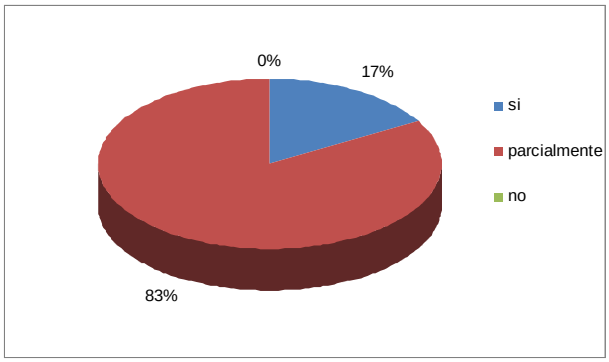
DS10: Administración de problemas

SI	PARCIALMENTE	NO
2	3	0



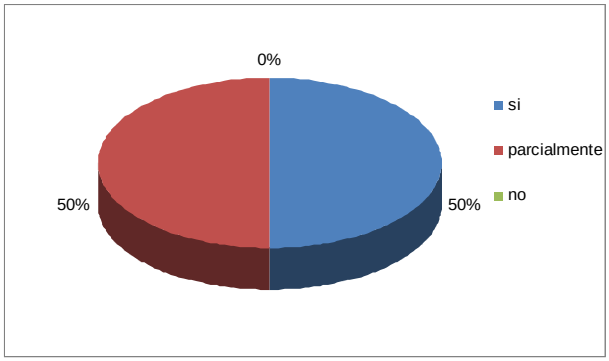
DS11: Administración de la Información

SI	PARCIALMENTE	NO
1	5	0



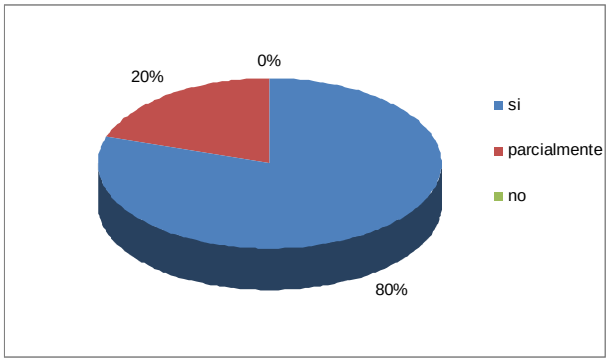
DS12: Administración del ambiente físico.

SI	PARCIALMENTE	NO
1	1	0



DS13: Administración de Operaciones

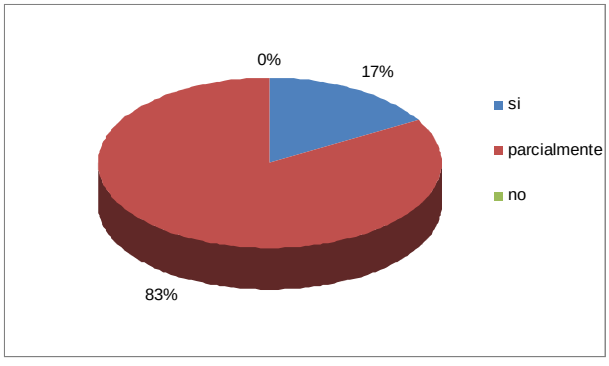
SI	PARCIALMENTE	NO
4	1	0



MONITOREAR Y EVALUAR

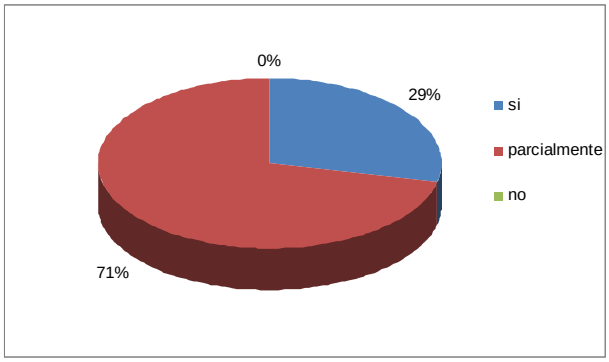
ME1: Monitorear y evaluar el desempeño de TI.

SI	PARCIALMENTE	NO
1	5	0



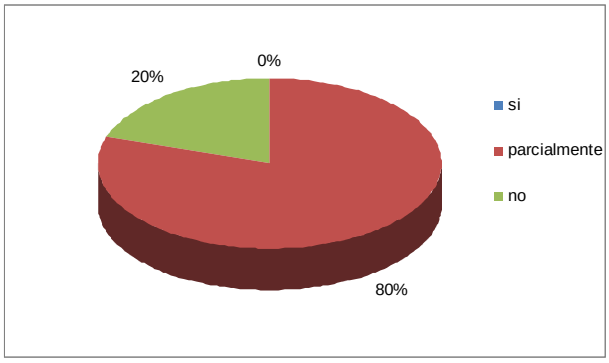
ME2: Monitorear y evaluar el control interno.

SI	PARCIALMENTE	NO
2	5	0



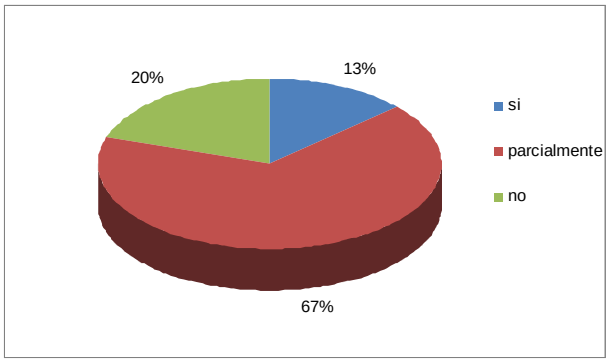
ME3: Garantizar el cumplimiento regulatorio.

SI	PARCIALMENTE	NO
0	4	1



ME4: Proporcionar Gobierno de TI.

SI	PARCIALMENTE	NO
2	10	3



ANEXO 6: CARTA ENTREGADA POR LA EMPRESA CASO ESTUDIO