
ESCUELA POLITECNICA DEL EJERCITO

VICERRECTORADO DE INVESTIGACION Y VINCULACION CON LA COLECTIVIDAD

MAESTRÍA EN GERENCIA DE SISTEMAS X PROMOCIÓN
PROYECTO DE INVESTIGACION PRESENTADO PREVIO A LA OBTENCION DEL TITULO DE MAGISTER EN GERENCIA DE SISTEMAS

# AUDITORIA DE RIESGOS INFORMÁTICOS DEL DEPARTAMENTO DE SISTEMAS DE CAVES SA EMA UTILIZANDO COBIT COMO MARCO DE REFERENCIA

INGENIERO JORGE GEOVANNI AUCANCELA SOLIZ

SANGOLQUI, OCTUBRE 2012

# CERTIFICACION DEL DIRECTOR

Certifico que el presente trabajo titulado: "AUDITORIA DE RIESGOS INFORMÁTICOS DEL DEPARTAMENTO DE SISTEMAS DE CAVES SA EMA UTILIZANDO COBIT COMO MARCO DE REFERENCIA", fue realizado en su totalidad por el Ingeniero Jorge Geovanni Aucancela Soliz, bajo mi supervisión, y cumple con las normas estatuarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Escuela Politécnica del Ejército.

Sangolquí, 25 de Octubre 2012

_____

Ing. Giovanni Roldan Crespo.
Director del Proyecto.

# DECLARACION

La Tesis de Grado Titulada, **Auditoria de Riesgos Informáticos del Departamento de Sistemas de Caves Sa. Ema. Utilizando COBIT Como Marco De Referencia**, ha sido desarrollada en base a una investigación, respetando derechos intelectuales de terceros, cuyas fuentes son citadas e incorporadas en la bibliografía.

En Virtud de esta declaración me responsabilizo del contenido, veracidad y alcance científico de esta tesis.

Sangolquí, 25 de Octubre del 2012

_____

Ing. Jorge Geovanni Aucancela Soliz

# AUTORIZACION

Yo, Jorge Geovanni Aucancela Soliz, con CI: 0602388365, Autorizo a la Escuela Politécnica del Ejercito, la publicación en la Biblioteca virtual, el Proyecto de Tesis de mi autoría titulada **Auditoria de Riesgos Informáticos del Departamento de Sistemas de Caves Sa Ema Utilizando Cobit Como Marco De Referencia**. cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, 25 de Octubre del 2012

_____

Ing. Jorge Geovanni Aucancela Soliz

# AGRADECIMIENTOS

Un reconocimiento muy especial al Ing. Giovanni Roldan, Director de Tesis, por su incondicional apoyo, y su aporte profesional en toda la elaboración del presente Proyecto.

Mis sinceros Agradecimientos a los Profesores de la Maestría Gerencia en Sistemas X promoción por sus valiosos conocimientos impartidos, en especial al Ing. Carlos Procel MSc., coordinador del programa, por su preocupación y desinteresada colaboración.

Jorge Geovanni Aucancela Soliz

# DEDICATORIA.

A mis mágicas Princesas, Anahí y Valentina, que con su amor y ternura me inspiraron a subir un peldaño más en mi vida, perdón por utilizar su tiempo

A mi bella Esposa, Verónica, por su apoyo incondicional, por empujarme cuando creía que era imposible lograr esta meta.

A mis Padres, y Herman@s, gracias por ser mi inspiración, que Dios bendiga nuestra linda Familia.

Geovanni.

# INDICE DE CONTENIDOS.



## CAPITULO 1

## CAPITULO 2



## CAPITULO 3

## CAPITULO 4

## CAPITULO 5

# INDICE DE TABLAS.

# INDICE DE FIGURAS.

# RESUMEN

El presente proyecto tiene por objeto realizar la auditoría de la empresa CAVES SA EMA, y establecer el Nivel de Madurez en que se encuentra, para lo cual se utilizó el modelo COBIT planteado por ISACA.

Se inicia con una Introducción al proyecto, en donde se describen los Objetivos y la importancia del desarrollo del presente trabajo. Seguidamente se detalla la metodología COBIT a utilizar para el desarrollo de la Auditoria, adicionalmente se realiza la identificación de los Procesos críticos del negocio mediante un análisis de la Empresa, identificando su cultura organizacional, el Ambiente Interno y Externo, Procesos, Inventario de Procesos soportados por TI.

Se establece dos formas para selección de Procesos COBIT a Auditar, la primera, a través de Enlaces entre los Procesos Críticos identificados con las Metas del Negocio, Metas y procesos de TI establecidas por COBIT, y la segunda, por medio de matrices o encuestas que propone ISACA en su libro “Cobit Implementation Tool Set". Mediante la evaluación a las dos formas de selección se obtiene los Procesos Cobit a Auditar.

A continuación se procede a desarrollar la auditoría, bajo la siguiente estructura: Obtención de entendimiento, Evaluación de Controles ,Indicadores Claves de Rendimiento, Nivel de Madurez determinado

Finalmente se culmina con la definición de niveles de madurez e impacto en el negocio, estableciendo las Recomendaciones y Plan de Acción que deberá poner en Marcha la empresa.

# ABSTRACT

This project aims to audit the company CAVES SA EMA, and establish the level of maturity that is found, for which we used the model proposed by ISACA COBIT.

It begins with an introduction to the project, which describes the objectives and importance of the development of this work. Following detailed COBIT methodology used for the conduct of the audit, performed additionally identifying the critical business processes through an analysis of the Company, identifying their organizational culture, the internal and external environment, Processes, Processes Inventory Supported by IT.

It provides two ways for selecting COBIT processes to audit, the first, through links between identified critical processes with business goals, IT goals and processes established by COBIT, and second, through surveys matrices or ISACA proposes in his book "Cobit Implementation Tool Set." by evaluating the two forms of selection is obtained COBIT processes audited.

Then we proceed to develop the audit, under the following structure: Obtaining understanding Controls Testing, Key Performance Indicators, given Maturity Level

Finally it ends with the definition of maturity levels and impact on the business, establishing the Recommendations and Plan of Action to be starting the company.

## ANTECEDENTES

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada.

La empresa CAVES SA EMA ha entendido que , la información y la tecnología que las soporta, representan uno de sus activos más valiosos, la causa fundamental es que la empresa han sufrido un cambio importante en sus procesos de negocio al considerar a la información como un recurso de importancia estratégica. Ello requiere, que igual que para el resto de los activos de la empresa los requisitos de eficacia y eficiencia, dentro de un marco de riesgos controlados, se apliquen a los Sistemas y Tecnologías de la Información

Para ello la Empresa desde hace algún tiempo a tenido la necesidad de implementar un método de control o auditoria informática para tener una dimensión concreta del área de sistemas, de sus debilidades y fortalezas, para que con un informe se pueda establecer los pasos y procesos para mejorar continuamente.

Es importante también la identificación de los riesgos que podrían amenazar la infraestructura tecnológica y sobre todo a la información, es primordial considerar la ejecución de una auditoría de riesgos informáticos, basada en los estándares internacionales adecuados, que permitan evaluar la situación actual y generar planes que permiten actuar de forma rápida ante cualquier eventualidad. Otorgar seguridad en el manejo de la información y a la

estructura tecnológica adyacente, es la principal premisa que se busca alcanzar con la elaboración de una auditoría de riesgos informáticos.

El presente proyecto de titulación tiene por objeto realizar la auditoría de Riesgos Informáticos de la empresa CAVES SA EMA, para establecer el Nivel de Madurez en que se encuentra, y finalmente recomendar y plantear proyectos para que la empresa pueda mejorar su nivel de Madurez, para lo cual utilizaremos el estándar COBIT como marco de referencia.

**DESCRIPCIÓN DEL DOCUMENTO**

Este proyecto de titulación está conformado por varios capítulos y anexos que se describen a continuación:

El Capitulo I, JUSTIFICACIÓN DEL USO DE COBIT COMO MARCO DE REFERENCIA, el uso de COBIT como marco de referencia, utilizada como herramienta para la ejecución de la Auditoria.

A continuación se realiza la identificación de los Procesos críticos del negocio para lo cual se inicia con una Definición de la Empresa, identificando su cultura organizacional, el Ambiente Interno y Externo, Procesos, Inventario de Procesos soportados por TI.

El Capítulo II, SELECCIÓN DE LOS PROCESOS A SER AUDITADOS, define los Procesos COBIT a ser auditados mediante dos formas: Primero por la Selección de los procesos mediante la relación de procesos críticos del negocio y las metas del negocio propuestos por COBIT, y segundo por medio de matrices o encuestas que propone ISACA en su libro “Cobit

Implementation Tool Set. Mediante la ponderación a las dos formas de selección se obtiene los Procesos Cobit a Auditar.

El Capítulo III, EJECUCION DE LA AUDITORIA, Desarrollo de la auditoría, bajo el siguiente estructura: Obtención de entendimiento, Evaluación de Controles ,Indicadores Claves de Rendimiento, Nivel de Madurez determinado, como resultado final se presenta los Resultados de la Auditoría en donde se define los niveles de madurez e impacto en el negocio, estableciendo los Planes de Acción que deberá poner en Marcha la empresa. Descripción de Proyectos que permitan disminuir la brecha existente entre el nivel de madurez actual, y el Objetivo definido.

El Capítulo 4 describe los Proyectos de Inversión, cuya ejecución permitirá disminuir la brecha existente entre el Nivel de Madurez actual, con el Nivel de Madurez Objetivo.

Finalmente en el El Capitulo V: Describe las Conclusiones y Recomendaciones

## JUSTIFICACIÓN METODOLÓGICA

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes.

COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares, por lo que COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque que se encuentra orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de TI.

Los beneficios de implementar COBIT como marco de referencia de gobierno sobre TI incluyen:

- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia, de lo que hace TI
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores
- Entendimiento compartido entre todos los participantes, con base en un lenguaje común
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI.

## DEFINICIÓN DEL PROBLEMA

El área de sistemas de la empresa al momento está constituido por 1 Gerente de Sistemas, 1 Jefe de Sistemas, y 2 Ingenieros de Sistemas, que realizan las actividades de supervisión y soporte en los diferentes campos de operación con que cuenta la empresa.

Se han identificado algunos problemas relacionados con los procesos, ya que no existe una correcta documentación de las actividades diarias, creando conflictos al momento de resolver problemas, por lo general estos son resuelto de manera reactiva, también influye el hecho de manejar las operaciones en diferentes lugares y esto genera que no se manejan algunas procedimientos de manera uniforme.

CAVES SA EMA, como todas las empresas se ha vuelto cada vez más dependiente de la tecnología para manejar sus actividades de forma ágil y correcta, la disponibilidad de los sistemas informáticos se ha vuelto un aspecto crucial. Actualmente, se necesita un alto y continuo nivel de disponibilidad, ya que resultaría extremadamente difícil funcionar sin los recursos informáticos

Estas son las razones entre otras por las que se hace muy necesario implementar un plan de auditoría en el área de sistemas de la empresa, con el fin de establecer lineamientos para que en el futuro puedan implementar y estandarizar procesos y procedimientos que no se los tenía antes, con el fin de mejorar el orden que se tiene al momento e incrementar la productividad y efectividad del área

*OBJETIVOS*

*Objetivo general*

Evaluar la situación actual del Departamento de Sistemas de CAVES SA EMA utilizando COBIT como marco de referencia, y presentar un informe con conclusiones y recomendaciones a la alta gerencia en base a la auditoría realizada, para minimizar los riesgos informáticos y conseguir incrementar la satisfacción de los usuarios de los sistemas automatizados.

*Objetivos específicos*

- Aplicación del marco de Referencia COBIT para realizar la auditoría
- Uso de los modelos de madurez y una metodología propuesta por COSO para modelar el impacto de los objetivos de control sobre los recursos y criterios de TI.
- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Incrementar la satisfacción de los usuarios de los sistemas computarizados
- Presentar alternativas de Proyectos a corto mediano y largo plazo que permitirán asegurar una mayor integridad, confidencialidad y confiabilidad de la información
- Minimizar existencias de riesgos en el uso de Tecnología de información
- Decisiones de inversión y gastos innecesarios con Justificación financiera de recomendaciones de compra de equipos o software.

## META DEL PROYECTO

Presentar un informe final con recomendaciones a la alta gerencia con el fin de mejorar o llegar a un correcto nivel de control interno en la empresa, con lo que está relacionado con el área de tecnología, todo esto para mejorar la eficacia operacional y administrativa, además de llegar a determinar una relación correcta entre costo beneficio de sistemas automatizados en la empresa, todo esto se lo hace para mejorar la satisfacción de los usuarios con respecto al área de informática, para ello es necesario el conocimiento claro del papel del departamento dentro de la empresa.

*METODOLOGÍA DE TRABAJO A UTILIZARSE*

Para el presente proyecto, se utilizará COBIT como marco de Referencia para realizar la auditoría.

COBIT se enfoca en qué se requiere para lograr una administración y un control adecuado de TI, y se posiciona en un nivel alto. COBIT ha sido alineado y armonizado con otros estándares y mejores prácticas más detallados de TI.

# CAPITULO I

## BASE CONCEPTUAL

### 1.1 COBIT COMO MARCO DE REFERENCIA

En la actualidad existe una variedad de lineamientos y mejores prácticas para el control y administración de la tecnología de información; algunos de ellos, han ido madurando a través del tiempo hasta convertirse en verdaderos estándares de uso obligado dentro de la gestión de TI.

La mayoría de los estándares y guías más conocidos o utilizados se basan en las "prácticas aceptadas" de las organizaciones y expertos de tecnología de información; lo cual, significa que están desarrolladas de acuerdo a la realidad de las organizaciones y que ya han sido probadas con éxito en empresas exitosas a nivel mundial. Esto garantiza la disposición de herramientas eficaces para la implementación de los Sistemas de Control y Seguridad informática por parte de los profesionales y auditores de TI.

La empresa requiere auditar los procesos críticos del negocio que representan un pilar fundamental para el buen funcionamiento de CAVES SA EMA, razón por la cual en el presente proyecto se utilizará COBIT como Marco de Referencia para el desarrollo de la Auditoria Planteada, que es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización.

### 1.1.1 INTRODUCCION A COBIT.

COBIT – Objetivos de Control para la Información y Tecnologías Afines (Control Objetives for Information and related Technology).

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders). COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares.

La última versión, COBIT® 4.1, enfatiza el cumplimiento normativo, ayuda a las organizaciones a incrementar el valor de T.I., apoya el alineamiento con el negocio y simplifica la implantación de COBIT. Esta versión no invalida el trabajo efectuado con las versiones anteriores del COBIT, sino que puede ser empleado para mejorar el trabajo previo.

Cuando importantes actividades son planeadas para iniciativas de Gobierno de TI, o cuando se prevé la revisión de la estructura de control de la empresa, es recomendable empezar con la más reciente versión de COBIT.

COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de

procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma.

Beneficios de implementar COBIT como un marco de referencia de Gobierno de TI:

- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia, de lo que hace TI
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI.

## 1. 1.2 MARCO DE TRABAJO DE COBIT

### Misión

Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en TI con autoridad, actualizados, de carácter internacional, y aceptados generalmente para el uso cotidiano de gerentes de empresas u organizaciones y auditores.

### Enfocándose en los procesos.

En la figura 1.1 se ilustra el Marco de Trabajo General de COBIT por un modelo que divide TI en 34 procesos alineados con las áreas de responsabilidad de planificación, desarrollo, operación y monitoreo, proveyendo una visión de principio a fin (end-to-end) de TI.

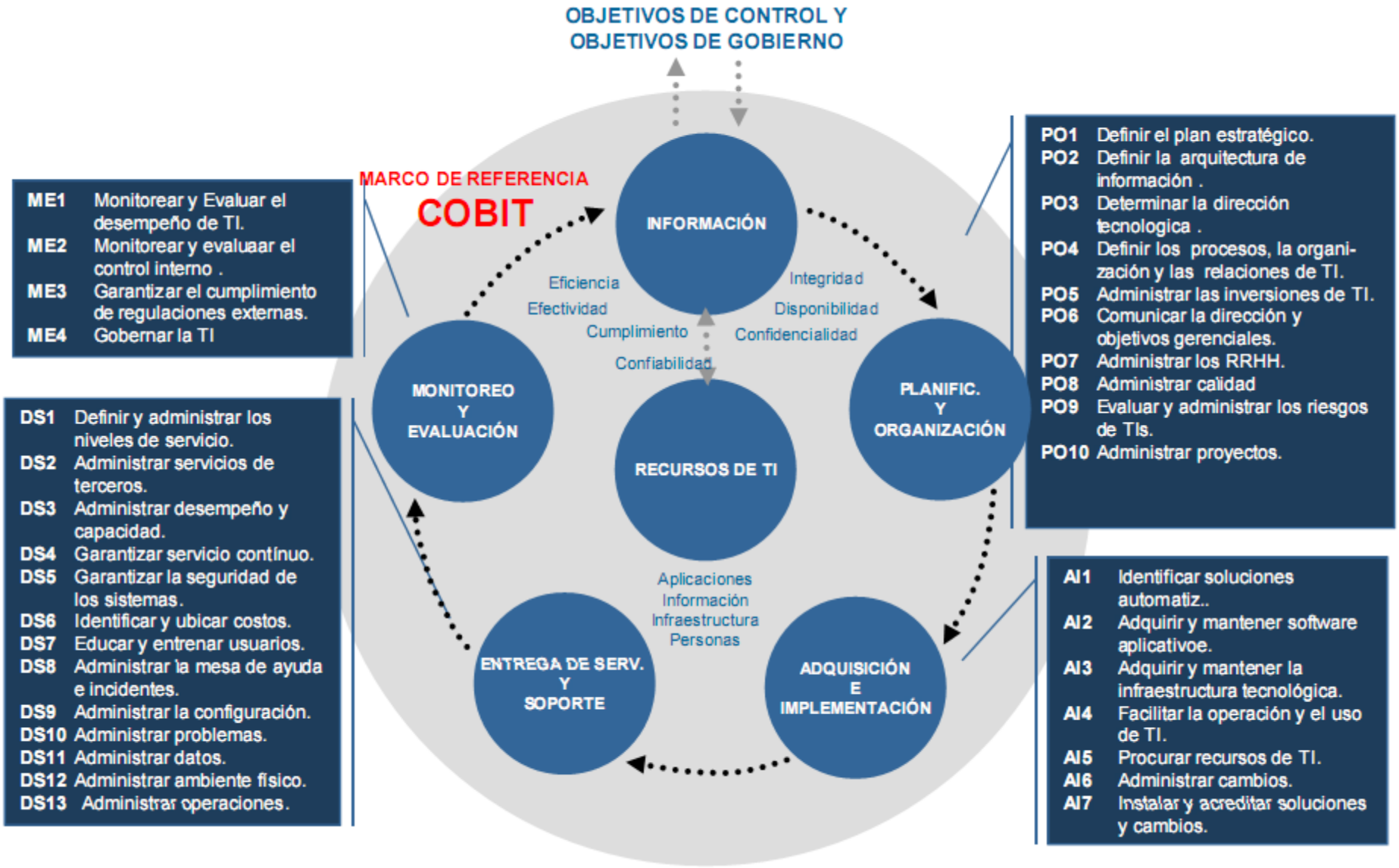



Figura 1.1: Marco de Trabajo General de COBIT

COBIT define las actividades de TI en un modelo de procesos genéricos con cuatro dominios:

**PLANEAR Y ORGANIZAR (PO)**

Este dominio cubre estrategias y tácticas, y se preocupa en identificar la manera en que TI puede contribuir mejor a alcanzar los objetivos de negocios.

**ADQUIRIR E IMPLEMENTAR (AI)**

Para realizar la estrategia de TI, se necesita identificar soluciones de TI así como también implementarlas e integrarlas en el proceso de negocio.

**ENTREGAR Y SOPORTAR (DS)**

Este dominio trata de la entrega real de los servicios requeridos, lo cual incluye entrega, gestión de seguridad y continuidad, soporte de servicio, y gestión de datos y suministros operativos

**MONITOREAR Y EVALUAR (ME)**

Este dominio trata de la gestión de funcionamiento, monitoreo de control interno, conformidad regulatoria y gobierno del aprovisionamiento.

### 1.1.3 OBJETIVOS DE CONTROL DE LOS PROCESOS

El control está definido como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proveer con una seguridad razonable que los objetivos de negocios serán alcanzados.

Los objetivos de control de COBIT son los requerimientos mínimos para el control efectivo de cada proceso de TI.

COBIT provee un modelo de procesos genérico que representa todos los procesos normalmente encontrados en funciones de TI, proporcionando un modelo de referencia común entendible para los gestores operativos de TI y a los gestores de negocios.

Puesto que los objetivos de control de TI de COBIT están organizados mediante procesos de TI, el marco de referencia provee un vínculo claro entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

El Marco de Referencia de Control COBIT contribuye a la necesidad de controlar la entrega satisfactoria de los servicios de TI en función de los objetivos de negocios:

- Vinculando TI a los requerimientos de negocios
- Organizando las actividades de TI en un modelo de proceso generalmente aceptado

- Identificando los principales recursos de TI a ser enfatizados
- Definiendo los objetivos de control de gestión a ser considerados.

### 1.1.4 INTERRELACIONES DE LOS COMPONENTES COBIT

Los recursos de TI están gestionados por los procesos de TI para alcanzar las metas de TI que responden y se alinean a los requerimientos de negocios.

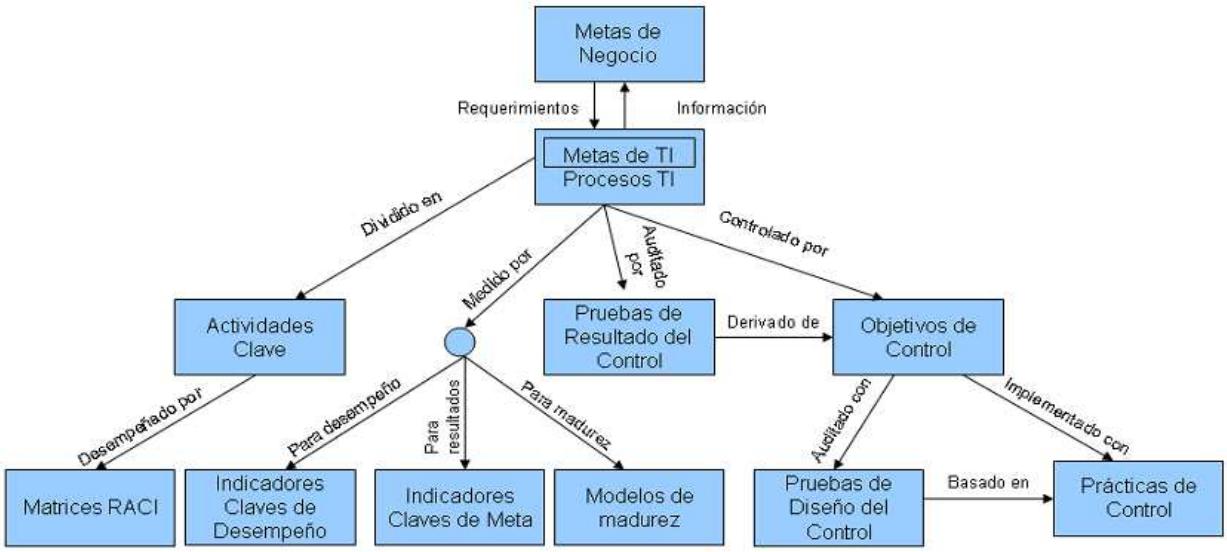



**Figura 1.2: Interrelaciones componentes COBIT**

### Orientación a los negocios de COBIT

***Consiste en:***

- Vincular las metas de TI las metas de negocio
- Proveer métricas y modelos de madurez para el logro de los mismos

- Identificar las responsabilidades de negocio y los dueños de los procesos de TI asociados.

### 1.1.5 METAS DE NEGOCIO Y METAS DE TI.

- La definición de un conjunto de metas genéricas de negocios y TI provee una base más refinada para establecer requerimientos de negocios y desarrollar las métricas que permitan la medición contra estas metas.
- Cada empresa usa TI para soportar iniciativas de negocios y estas pueden estar representadas como metas de negocio para TI
- Si TI va a entregar exitosamente servicios para soportar la estrategia de la empresa, debería haber una propiedad y dirección claras de los requerimientos para el negocio (el cliente) y un claro entendimiento de qué necesita ser entregado y como por parte de TI (el proveedor).

Las empresas exitosas entienden los riesgos, explotan los beneficios de TI, y encuentran modos para tratar de:

- Alinear la estrategia de TI con la estrategia del negocio
- Ir transmitiendo y conectando la estrategia de TI y las metas hacia abajo en la empresa
- Proveer estructuras organizacionales que faciliten la implementación de estrategias y metas
- Crear relaciones constructivas y comunicaciones efectivas entre los negocios y TI, y con socios externos

- Medir funcionamientos de TI.

Las áreas de TI no pueden hacer una entrega eficaz en función de los objetivos de negocios y los requerimientos de gobierno sin adoptar e implementar un marco de referencia de gobierno y control de TI para:

- Hacer un vínculo a los requerimientos de negocio
- Hacer que el funcionamiento sea transparente en función de esos requerimientos
- Organizar sus actividades en un modelo de procesos generalmente aceptado
- Identificar los recursos principales a ser potenciados
- Definir los objetivos de control de gestión a ser considerados

Las mejores prácticas de TI se han vuelto significativas por un número de factores:

- Los gestores de negocio y directores demandan un mejor retorno de las inversiones de TI
- La preocupación sobre el generalmente creciente nivel de gastos de TI
- La necesidad de cumplir requerimientos regulatorios para controles de TI en áreas tales como privacidad y reportes financieros, y en sectores específicos tales como finanzas, industria farmacéutica y salud
- La selección de proveedores de servicio y la gestión del outsourcing de servicios y compras
- Riesgos, relacionados con TI, crecientemente complejos tales como seguridad de redes.

- Iniciativas de gobierno de TI que incluye la adopción de marcos de referencia de control y mejores prácticas para ayudar a monitorear y mejorar actividades críticas de TI para incrementar el valor del negocio y reducir los riesgos del mismo
- La necesidad de optimizar costos siguiendo, si es posible, aproximaciones estándares en lugar de desarrollos especiales
- La creciente madurez y consecuente aceptación de marcos de referencia bien considerados como COBIT, ITIL, ISO 17799, ISO 9001, CMM
- La necesidad de las empresas de evaluar cómo están respecto de estándares generalmente aceptados y respecto a sus pares.

**Como se asegura la empresa que TI alcanza los objetivos y soporta el negocio?**

- Definiendo objetivos de control que aseguren que:
    - Se alcancen los objetivos de negocio
    - Se prevengan o detecten y corrijan eventos indeseados
- Estableciendo y monitoreando los controles y niveles de funcionamiento de TI apropiados mediante:
    - Mediciones (Benchmarking) de capacidad de proceso de TI expresada como modelos de madurez.
    - Metas y Métricas de los procesos de TI para definir y medir sus resultados y funcionamiento (Balanced ScoreCard)

- Metas de Actividad para tener estos procesos bajo control (COBIT)

**Importancia de un Marco de Referencia de Control para el Gobierno de TI.**

- Cada vez más la alta dirección percibe el impacto significativo que la información puede tener en el destino de la empresa.
- La alta dirección necesita conocer si la TI está siendo gestionada de manera que esta es:
  - Adecuada para alcanzar los objetivos
  - Suficientemente flexible para aprender y adaptarse
  - Consecuente en la gestión de los riesgos que enfrenta
  - Apropiada reconociendo oportunidades y actuando sobre ellas.

**Quienes necesitarían de un Marco de Referencia de Control para el Gobierno de TI.**

Un marco de referencia de gobierno y control necesita servir a una variedad de actores internos y externos:

- Accionistas dentro de la empresa quienes tienen un interés en generar valor de las inversiones de TI:
  - Aquellos que toman decisiones de inversión
  - Aquellos que deciden sobre requerimientos
  - Aquellos que usan los servicios de TI.

- Accionistas internos y externos que proveen servicios de TI:
    - Aquellos que gestionan la organización y los procesos de TI
    - Aquellos que desarrollan capacidades
    - Aquellos que operan los servicios
- Accionistas internos y externos que tienen responsabilidades de control/riesgos:
    - Aquellos con responsabilidades de seguridad, privacidad y/o riesgos
    - Aquellos que realizan funciones de aprobación
    - Aquellos que requieren o proveen servicios de garantía.

### 1.1.6 CRITERIOS DE INFORMACIÓN DE COBIT.

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

- **Eficacia:** Información relevante a los procesos de negocios y su entrega en tiempo, correcta, consistente y usable.
- **Eficiencia:** Provisión de información a través del óptimo uso de los recursos.
- **Confidencialidad:** Protección de información sensible contra acceso no autorizado

- **Integridad:** Exactitud y completitud de la información y su validez de acuerdo a los valores y expectativas de negocio.
- **Disponibilidad:** Que la información esté disponible cuando sea requerida por el proceso de negocios ahora y en el futuro.
- **Conformidad:** Se ocupa de cumplir con las leyes, regulaciones y contratos a los cuales se sujeta el proceso de negocios.
- **Confiabilidad:** Provisión de información apropiada a la gerencia para operar la organización.

### 1.1.7 RECURSOS DE TI

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio.

Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una capacidad técnica adecuada (Ej., un sistema de planeación de recursos empresariales) para dar soporte a la capacidad del negocio (Ej., implementando una cadena de suministro) que genere el resultado deseado (Ej., mayores ventas y beneficios financieros)

Los recursos de TI identificados en COBIT se pueden definir como sigue:

- **Aplicaciones:** incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- **Información:** son los datos en todas sus formas de entrada, procesados y generados por los sistemas de información, en cualquier forma en que son utilizados por el negocio.
- **Infraestructura:** es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- **Personas:** son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

En la siguiente tabla se muestra el impacto de los objetivos de control COBIT sobre los recursos y criterios de TI. En los recursos de TI una X significa que ese objetivo de control tiene impacto sobre el recurso y un espacio en blanco que no tiene impacto. En los criterios de información se identifica el grado de impacto; Primario (P), para indicar impacto directo sobre el criterio de información, Secundario (S) impacto indirecto o en menor medida y espacio en blanco o vacío, que no tiene impacto alguno.

**Tabla 1.1: Impacto de los objetivos de control COBIT sobre los recursos y criterios de TI**

| DOMINIO | | PROCESOS DE TI | Criterios de Información | | | | | | | Recursos de TI | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Efectividad | Eficiencia | Confidencialidad | Integridad | Disponibilidad | Cumplimiento | Confiabilidad | Recursos humanos | Sistemas de información | Tecnología | Instalaciones | Datos |
| Planeación y Organización | PO1 | Definir un Plan Estratégico de TI | P | S | | | | | | X | X | X | X | X |
| | PO2 | Definir la Arquitectura de Información | P | S | S | S | | | | | X | | | X |
| | PO3 | Definir la Dirección Tecnológica | P | S | | | | | | | | X | X | |
| | PO4 | Definir la Organización y las Relaciones de TI | P | S | | | | | | X | | | | |
| | PO5 | Administrar la Inversión de Tecnología de Información | P | P | | | | | S | X | X | X | X | |
| | PO6 | Comunicar las Aspiraciones y Dirección de la Gerencia | P | | | | | S | | X | | | | |
| | PO7 | Administrar Recursos Humanos | P | P | | | | | | X | | | | |
| | PO8 | Asegurar el Cumplimiento con los Requerimientos Externo | P | | | | | P | S | X | X | | | X |
| | PO9 | Evaluar los Riesgos | S | S | P | P | P | S | S | X | X | X | X | X |
| | PO10 | Administrar Proyectos | P | P | | | | | | X | X | X | X | |
| | PO11 | Administrar Calidad | P | P | | P | | | S | X | X | X | X | |
| Adquisición e Implementación | AI1 | Identificar Soluciones Automatizadas | P | S | | | | | | | X | X | X | |
| | AI2 | Adquirir y Mantener Software de Aplicación | P | P | | S | | S | S | | X | | | |
| | AI3 | Adquirir y Mantener la Infraestructura Tecnológica | P | P | | S | | | | | | X | | |
| | AI4 | Desarrollar y Mantener los Procedimientos | P | P | | S | | S | S | X | X | X | X | |
| | AI5 | Instalar y Acreditar Sistemas | P | | | S | S | | | X | X | X | X | X |
| | AI6 | Administrar Cambios | P | P | | P | P | | S | X | X | X | X | X |
| Entrega de Servicios y soporte | DS1 | Definir Niveles de Servicio | P | P | S | S | S | S | S | X | X | X | X | X |
| | DS2 | Administrar los Sericios prestados por Terceras Partes | P | P | S | S | S | S | S | X | X | X | X | X |
| | DS3 | Administrar el Desempeño y la Capacidad | P | P | | | S | | | | X | X | X | |
| | DS4 | Asegurar el Servicio Continuo | P | S | | | P | | | X | X | X | X | X |
| | DS5 | Garantizar la Seguridad en los Sistemas | | | P | P | S | S | S | X | X | X | X | X |
| | DS6 | Identificar y Asignar Costos | | P | | | | | P | X | X | X | X | X |
| | DS7 | Educar y Capacitar Usuarios | P | S | | | | | | X | | | | |
| | DS8 | Atender y Aconsejar a los Clientes | P | | | | | | | X | X | | | |
| | DS9 | Administrar la Configuración | P | | | | S | | S | | X | X | X | |
| | DS10 | Administrar Problemas e Incidentes | P | P | | | S | | | X | X | X | X | X |
| | DS11 | Administrar Datos | | | | P | | | P | | | | | X |
| | DS12 | Administrar Instalaciones | | | | P | P | | | | | | X | |
| | DS13 | Administrar Operaciones | P | P | | S | S | | | X | X | X | X | X |
| Monitoreo | M1 | Monitorear los Procesos | P | S | S | S | S | S | S | X | X | X | X | X |
| | M2 | Evaluar qué tan adecuado es el Control Interno | P | P | S | S | S | S | S | X | X | X | X | X |
| | M3 | Obtener el Aseguramiento Independiente | P | P | S | S | S | S | S | X | X | X | X | X |
| | M4 | Colaborar en la Auditoría Independiente | P | P | S | S | S | S | S | X | X | X | X | X |

## 1.2 DEFINICION DE LA ORGANIZACIÓN.

CAVES S.A. EMA es una empresa de servicios de [1]catering y afines, constituida el 14 de Junio de 1991 en la ciudad de Quito, en el año 2003 CAVES CIA. Ltda. se asoció con el grupo GHL uno de los administradores hoteleros reconocidos a nivel mundial. Ahora con la experiencia de CAVES en catering petrolero y el amplio conocimiento del grupo GHL en administración hotelera, CAVES S.A. EMA es la primera compañía en el Ecuador que fusiona las dos ramas y brinda a sus clientes un servicio completo.

La empresa cuenta con una sede en Quito – Ecuador, Bogotá – Colombia y a partir de agosto del 2005 en Lima - Perú por lo que la administración de diversas facilidades de preparación y servicio de comidas y/o de albergues dentro de los países del área andina está dentro de su campo de operación, según lo contratado con los clientes. Adicionalmente CAVES - GHL, cuenta con un sistema de gestión de calidad que funciona en todos los campos en los que opera la compañía.

Se incluyen los servicios de preparación de alimentos y transporte de los mismos desde su planta de producción hasta el consumidor final, según la necesidad del cliente, abarcan además una amplia gama de servicios

[1] Servicio de alimentación institucional o alimentación colectiva que provee una cantidad determinada de comida y bebida, eventos y presentaciones de diversa índole.

adicionales entre los que se incluyen, pero no limitan a camarería, lavandería y servicios generales de mantenimiento de campamentos.

Es por esto que brinda la posibilidad a todos sus potenciales clientes de escoger entre diversas opciones de servicio, acordes al tipo de operación. Es una compañía con amplia experiencia en los servicios de catering a nivel de la industria petrolera y a nivel institucional y de gestión hotelera, razón por la cual está en capacidad de garantizar la satisfacción de todas las exigencias y necesidades de sus clientes.

El objeto social por el cual fue creada la compañía es el servicio de catering, exportación e importación de bebidas y concentrados con o sin alcohol y productos alimenticios para consumo humano, entre otros.

### 1.2.1 Cultura Organizacional

CAVES SA EMA, tiene una cultura organizacional basada en sus principios empresariales que están constituidos por su Misión, Visión y Valores, descritos a continuación.

- ***Misión.***

  Ser una empresa de reconocido prestigio, caracterizada por la alta calidad de sus productos y servicios en el área de catering, alimentación, camarería y lavandería. Garantizados por los lineamientos establecidos en su sistema de gestión de la calidad, en el marco de los requisitos contractuales y adicionales expresados explícita e implícitamente por cualquier organización pública o privada que solicite sus servicios.

- ***Visión***

Mantener y satisfacer las necesidades de sus clientes, y posicionarse como la empresa líder del sector de catering, con el mayor número de servicios de alimentación prestados a empresas de los diferentes sectores productivos del país, mediante:

- ✓ La calidad de sus productos y servicios, su versatilidad y tecnología.
- ✓ El alto profesionalismo de su personal, el cual es considerado el recurso principal dentro de la empresa.
- ✓ El uso de un sistema de Gestión de Aseguramiento de Calidad (ISO 9001) para sentar las bases para nuevos niveles de satisfacción del cliente.

- ***Valores.***
  - o Calidad Compromiso
  - o Cumplimiento
  - o Liderazgo
  - o Confiabilidad
  - o Respeto
  - o Trabajo en equipo
  - o Lealtad

### 1.2.2 CLIENTES

Están divididos en dos segmentos de mercado

- ✓ **Catering Petrolero**
- ✓ **Catering Institucional**

**CATERING PETROLERO**

Cubre empresas nacionales o extranjeras que se dedican a la explotación Petrolera o minera. La mayoría de las empresas están ubicadas en el oriente ecuatoriano.

**CATERING INSTITUCIONAL.**

Servicio de alimentación en empresas públicas y privadas, enfocándose principalmente en el sector bancario e industrial, de las ciudades de Quito y Guayaquil.

### 1.2.3 PRODUCTOS / SERVICIOS

Los servicios a los que se encuentra dirigida la empresa es el catering institucional y petrolero siendo este último el sector en el que predomina.

El servicio de catering petrolero comprende las siguientes actividades:

- ✓ Alimentos y bebidas
- ✓ Limpieza y arreglo de habitaciones
- ✓ Lavandería
- ✓ Limpieza de áreas públicas
- ✓ Transporte de comidas preparadas
- ✓ Mantenimiento de equipos
- ✓ Soporte Plan Nutricional
- ✓ Soporte Salud Ocupacional

La empresa presta el servicio, en cualquier situación geográfica que el cliente requiera.

### 1.2.4 LOS INVOLUCRADOS Y SUS EXPECTATIVAS

**Clientes**

Servicio de Calidad

Cumpliendo las normas y políticas propias

**Accionistas**

Rentabilidad

Imagen corporativa

**Empleados**

Estabilidad

Buen ambiente laboral

Remuneraciones Justas

**Proveedores**

Seriedad

Fidelidad

**Equipo directivo**

Cumplimiento de objetivos

**Gobierno**

Cumplimiento de obligaciones tributarias

Transparencia

**Sociedad**

Responsabilidad social

Generación de empleo

**Comunidad circunvecina**

Relaciones comunitarias

Otorgación de empleo a la comunidad

### 1.2.5 ANÁLISIS DEL AMBIENTE EXTERNO

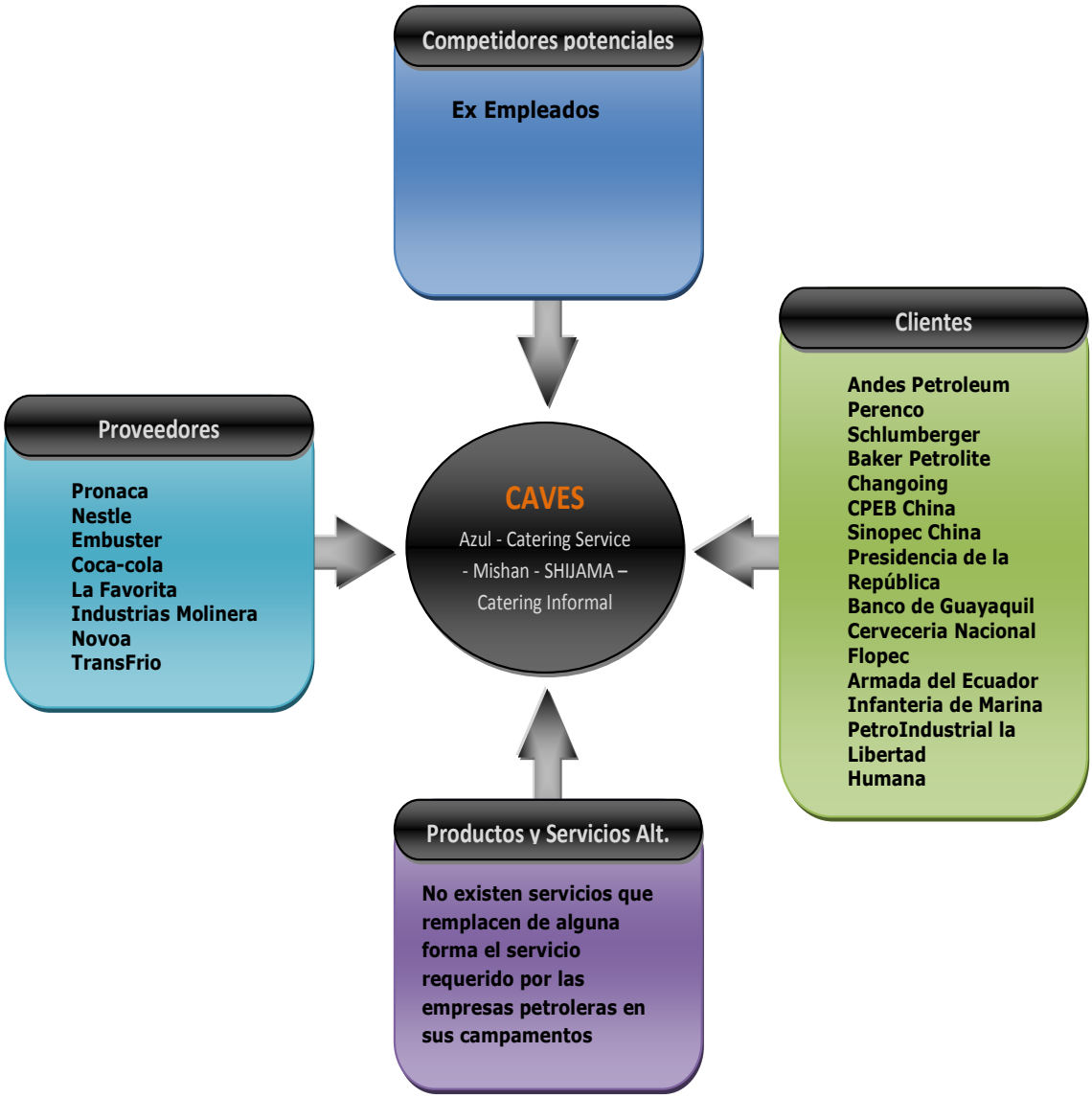



**Figura 1.3: Ambiente Externo de la Empresa**

**Competencia**

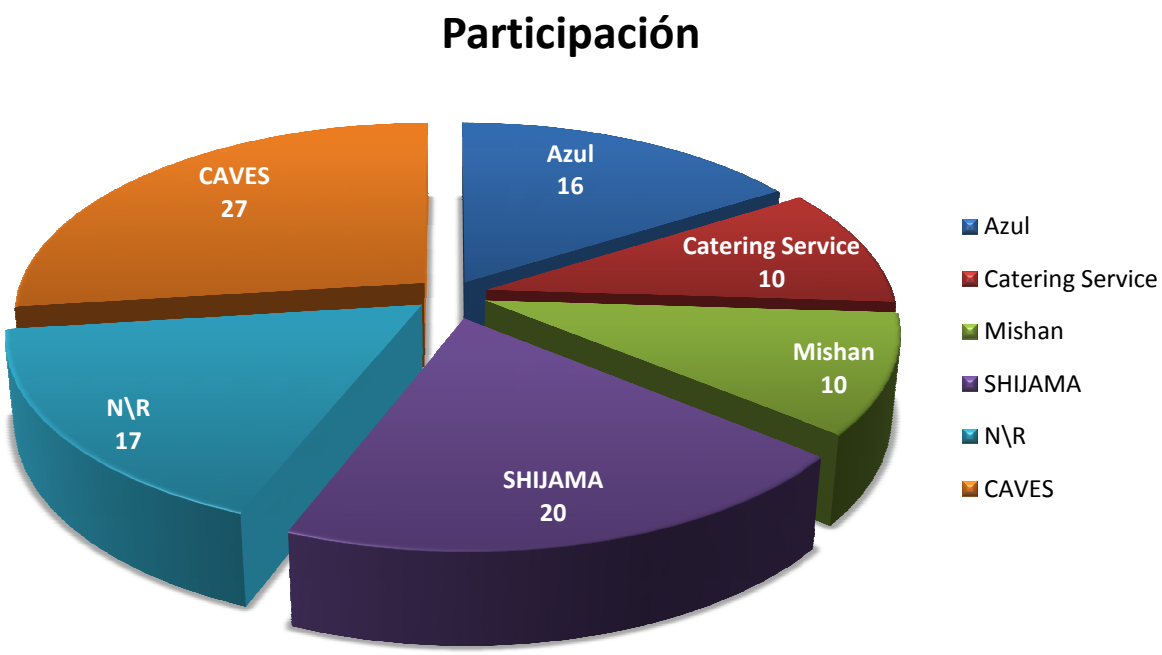



**Figura 1.4: Participación de la Competencia en el Mercado**

**Regulaciones (Leyes y reglamentos)**

CAVES S.A. fue constituida bajo las leyes y políticas del Estado ecuatoriano, regida por la *Ley de Compañías*, siendo la ***Superintendencia de Compañías*** su órgano rector.

Al ser una empresa legalmente constituida su manejo contable, financiero y tributario está basado en la *Ley de Régimen Tributario Interno* y su respectivo reglamento de aplicación.

Para la realización de sus actividades Caves S.A. se rige por el *Reglamento para la Aplicación del Mandato Constituyente Número 8* que suprime la tercerización de servicios complementarios.

**Políticas**

- Mantener un ambiente de trabajo seguro y libre de riesgos para los trabajadores, para lo que se propende a la creación de una cultura de seguridad en los trabajadores, ponderando la importancia de la prevención de riesgos, mediante difusión y capacitación permanente y la dotación de herramientas, equipos y ambientes libres de riesgos.

- Avalar la inocuidad en su producto final y la satisfacción del cliente, a través de la calidad de su servicio, y el cumplimiento de sus requisitos de Seguridad Alimentaria, se los declara como una responsabilidad de la Alta Dirección; por lo que, es el marco de referencia para el establecimiento y revisión de los objetivos medibles de la Institución.

- Mantener a nuestro cliente satisfecho por medio del permanente cumplimiento de sus requisitos, de las evaluaciones de su satisfacción y de la revisión permanente de los objetivos de calidad planteados en la empresa, para mantener un sistema de mejoramiento continuo.

### 1.2.6 ANÁLISIS DEL AMBIENTE INTERNO.

#### 1.2.6.1 CADENA DE VALOR DE CAVES SA EMA

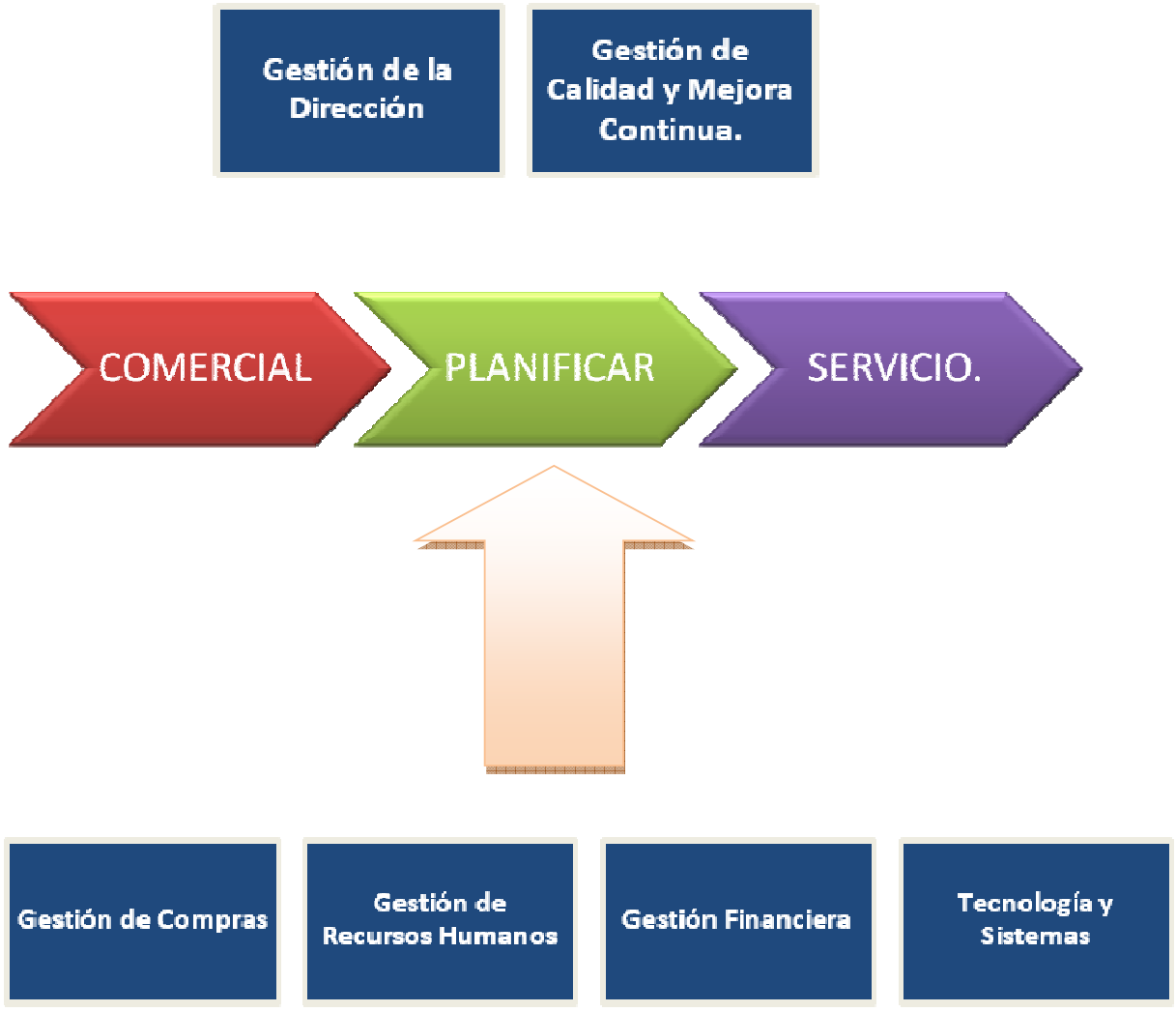



**Figura 1.5: Cadena de Valor CAVES SA EMA.**

**Proceso Central.**

Caves basa sus líneas de negocio, en proveer soluciones Hoteleros, a empresas del sector petrolero, en el lugar que este requiera.

**Actividades Primarias**

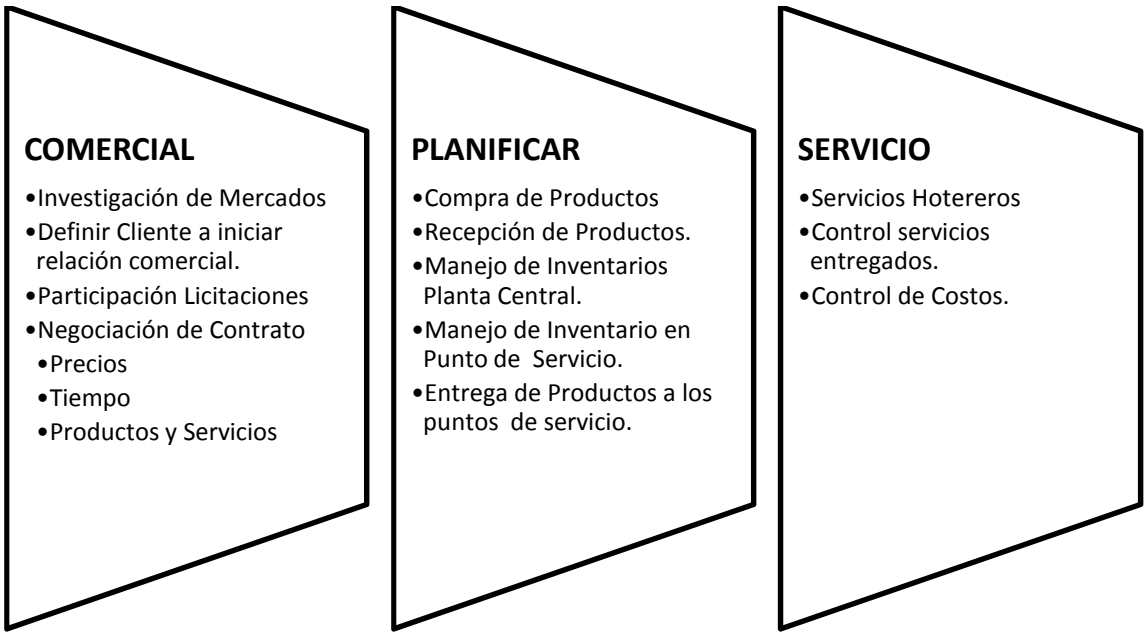



**Figura 1.6: Cadena de Valor - Actividades Primarias**

**ACTIVIDADES DE APOYO**

Las actividades primarias están apoyadas o auxiliadas por los diferentes Procesos que realizan los departamentos que integran la empresa:


**Figura 1.7: Cadena de Valor - Actividades de Apoyo**

### 1.2.7 ANALISIS FODA

**Oportunidades**

1. CAVES S.A EMA. brinda sus servicios utilizando su Sistema de Gestión Integrado, certificado bajo la norma ISO 9001: 2008.

2. Incentivos y premios para quienes cumplan con las metas estipuladas según el presupuesto de cada Campamento para mejorar la rentabilidad.

3. Alianzas estratégicas con proveedores claves para ofrecer productos y servicios de calidad.

4. Acceso a Mano de Obra y Materia Prima altamente calificada.

5. Demanda local e internacional de productos y servicios diferenciados y de calidad.

6. Tendencia modernizadora de catering a nivel de industria petrolera, nivel institucional y de gestión hotelera.

7. El servicio complementario que ofrece como la camarería, lavandería entre otros le permite obtener ventajas sobre sus competidores ya que estos no lo han desarrollado.

8. Amplio portafolio para brindar la posibilidad a todos sus potenciales clientes de escoger entre diversas opciones de servicio, acordes al tipo de operación.

**Amenazas**

1. Existe la posibilidad de que los empleados adquieran la experiencia necesaria y se transformen en futuros rivales de la organización.
2. La crisis económica ha hecho aparecer la competencia con mejores ofertas para los clientes.
3. El software que se utiliza, no cuenta con todas las licencias de uso.
4. Inestabilidad política, social e inseguridad jurídica.
5. Déficit Fiscal y en la Balanza Comercial.
6. Competencia desleal y no calificada.
7. El impacto de la Legislación en temas relacionados con los servicios complementarios ponen en riesgo la estabilidad de la empresa.
8. El cierre de campamentos petroleros disminuirá las ventas en esta área que es la fuente principal de ingresos.

**Fortalezas**

1. Existe un buen ambiente de trabajo y estabilidad laboral.
2. La empresa ha sido re certificada hasta la presente fecha con sus Sistema de Gestión Integrado de la Calidad, ISO 9001: 2008 / HACCP.
3. Plan de Optimización de Costos en base a los resultados y modificaciones realizadas a los años anteriores.
4. Seguridad Alimentaria, como factor clave de la Alta Dirección.
5. Personal con índices de cumplimiento que en promedio son del 85%.
6. Evaluación Permanente a través de índices de gestión de servicio.
7. Los productos desarrollados, constituyen una herramienta importante para la administración de los campos.
8. Selección de Personal Directivo de Experiencia.
9. Programa de capacitación anual de acuerdo a las necesidades del mercado.
10. Experiencia y prestigio en la administración de Catering.
11. Contar con la infraestructura y equipos para prestación de servicios de calidad.

**Debilidades**

1. Modificar el Procedimiento de Compras para simplificar el Proceso de Calificación de Proveedores.
2. Garantizar con mayor eficacia el cumplimiento de los requisitos para lograr calificar al 75% de los proveedores bajo el nuevo esquema de licitaciones.
3. El personal técnico tiene una evidente sobrecarga de trabajo que no necesariamente representa mejores ingresos.
4. El personal realiza múltiples funciones, no hay una clara delegación de funciones.
5. No existe planificación Estratégica.
6. Los Campamentos se manejan informalmente sin un sistema integrado.
7. No contar con una Investigación de Mercado anual sobre sus competidores.
8. Altos costos de producción y gastos administrativos.
9. El envío de productos cárnicos a los distintos campos no tiene un control adecuado por lo que existen muchos residuos aumentando el costo de ventas.
10. El costo de transporte de los alimentos desde la planta a los diferentes puntos de venta es muy alta ya que la empresa no cuenta con vehículos propios.
11. La empresa cuenta con un solo jefe de sistemas por lo que el alcance de solución de problemas técnicos e informáticos de los distintos campos es limitado.

### 1.2.8 ALINEAMIENTO ESTRATÉGICO

**Temas Estratégicos**

**Tabla 1.2: Relación Temas Estratégicos**

| No | Relación | Objetivos | Tema estratégico |
|---|---|---|---|
| 1 | F2 O1 | 1 | Manejo adecuado de políticas y estándares de calidad |
| 2 | F3 O4 | 1 | Excelencia de prestación de servicio |
| 3 | F4 F10 F11 | 3 | Trabajo con tecnología nueva, no contaminante, incluyente en la comunidad |
| 4 | D8 | 1 | Altos costos de producción para la prestación de servicios |
| 5 | D9 | 4 | Podrían darse problemas ambientales por la falta de control |
| 6 | F7 | 5 | Software in-house por lo que se ahorra costo de producción de sistemas y son a medida |
| 7 | D11 | 5 | Personal de tecnología insuficiente para abastecer a todos los campos |
| 8 | A2 | 2 | No hay manera de reducir mucho los costos por la calidad en procesos y productos |

**Objetivos - según Balanced Scorecard**

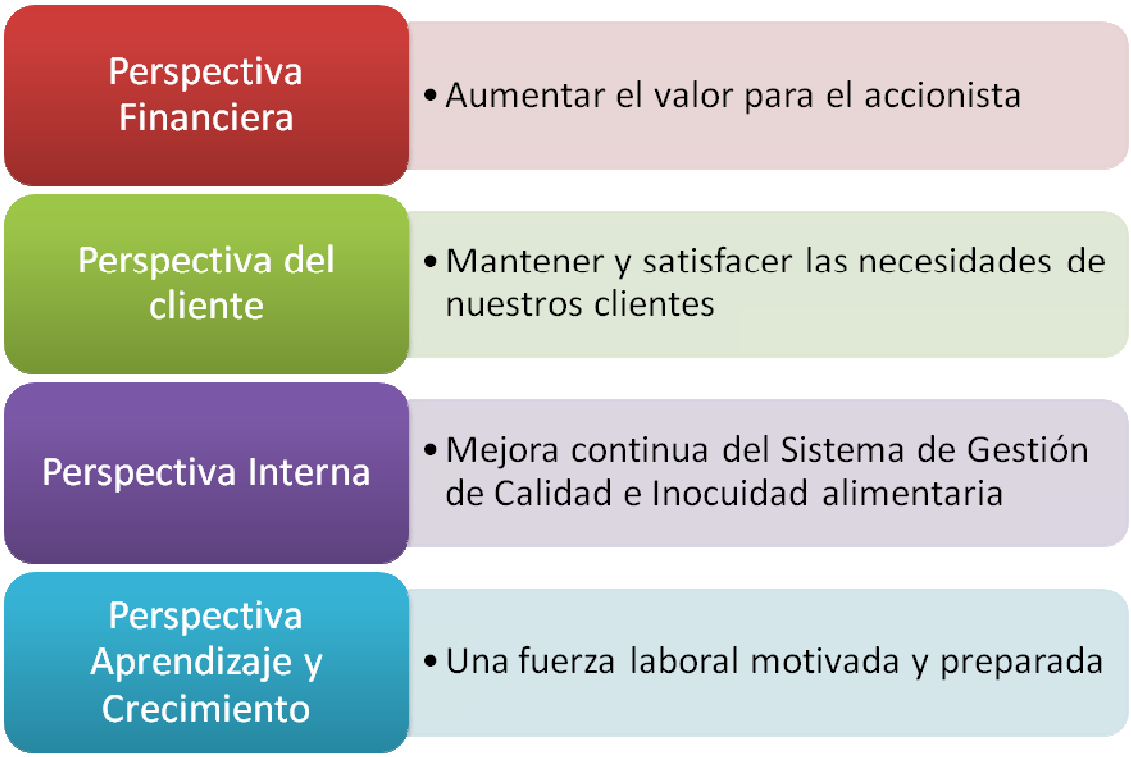



**Figura 1.8: Objetivos Empresa - Balanced Scorecard**

**Balanced Scorecard Empresa.**

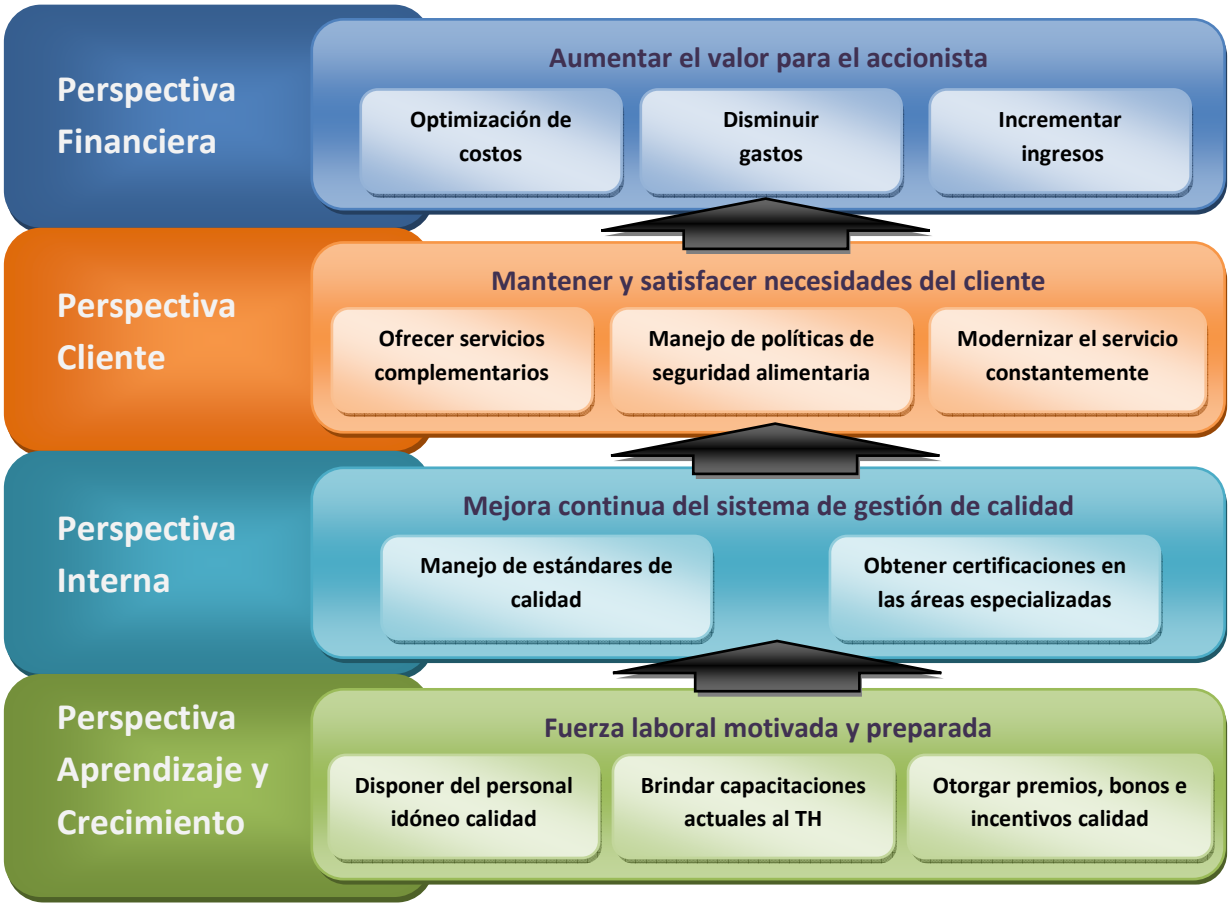



**Figura 1.9: Gráfico Causa Efecto - Balanced Scorecard**

### 1.2.9 PROCESOS CONCERNIENTES AL NEGOCIO

#### 1.2.9.1 Macroflujo del sistema de negocios de CAVES

Para establecer un modelo general del negocio de CAVE SA EMA basado en la Gestión por Mejora continua se ha diseñado un Macroflujo, en el cual se clasifican los Macroprocesos (M.P) y los procesos según el tipo de participación en el negocio, como de gestión, primarios y de apoyo.

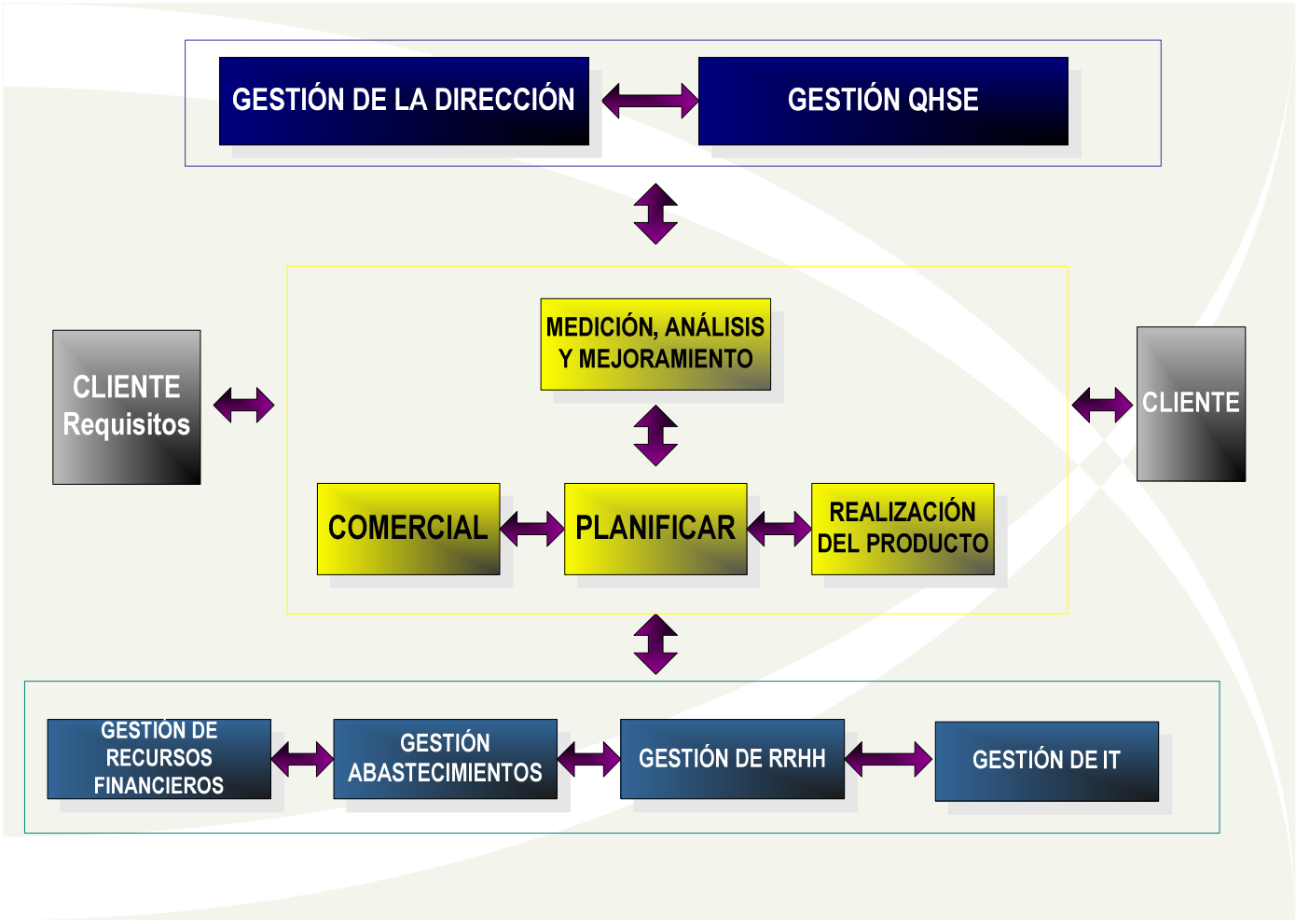



**Figura 1.10: Macroflujo del sistema de negocios de CAVES**

Este modelo parte desde las necesidades de las partes interesadas, con enfoque en los clientes, y muestra como fluye el negocio a través de la estructura de Macroprocesos (M.P) de CAVES hasta lograr la satisfacción de las mismas.

### 1.2.9.2 PROCESOS CLAVES.

Para concentrar los esfuerzos de mejoramiento de procesos, CAVES calificó a sus procesos según su influencia sobre los indicadores globales, determinando los “procesos clave” como los de mayor influencia y los “procesos importantes” los cuales le siguen en el orden de importancia. Los procesos “claves” e “importantes” son medidos y analizados a través de indicadores.

A continuación se detallan los procesos considerados Claves, identificando a que Macroproceso pertenece cada uno de estos:

**M.P: COMERCIAL**

**PRESENTACIÓN DE OFERTAS.**

Cumplimiento con especificaciones del cliente.

Evaluación de la capacidad de CAVES para cumplir con necesidades del Cliente.

Recepción de Ofertas por el cliente.

**Elaboración de Contratos.**

Confirmación de requisitos por el cliente.

Modificación de contratos.

**M.P: PLANIFICAR.**

**COMPRAS.**

Selección de Proveedores

Verificación de Precios.

Inspección de Entrada.

Despachos.

Evaluación de Proveedores.

**ABASTECIMIENTO DE PRODUCTOS.**

Inventarios

Envío / Recepción de Requisición.

**MANEJO DE INVENTARIO EN PUNTO DE VENTA.**

**Objetivo y Condiciones Necesarias:**

Mantener en stock la variedad y cantidad de productos suficiente para atender ágil y eficientemente lo requerimientos del cliente..

Las condiciones necesarias para ejecutar este proceso son:

- Materiales almacenados de manera ordenada visible y de fácil acceso
- Entrega oportuna y completa de los productos solicitados.
- Herramientas confiables para determinar el inventario óptimo y el punto de re-orden.

**EVALUACIÓN Y SELECCIÓN DE TRANSPORTE**

Selección de Compañía de Transporte

Evaluar Capacidad.

Determinar tipo de Transporte

**CARGA Y TRANSPORTE DE MERCADERÍAS.**

Inspección de Transporte.

Cargar el Vehículo

Evitar contaminación.

Ubicación adecuada de la carga

**M.P: REALIZACION DEL PRODUCTO**

**PREPARACIÓN Y ENTREGA DE COMIDAS Y AFINES.**

Aprobación del Menú

Orden de Producción.

Control de salida del producto final.

Control y entrega de comidas preparadas.

**M.P: FINANCIERO.**

**Cobranzas.**

**Objetivos y Condiciones Necesarias:**

Recuperar cartera en forma oportuna de acuerdo a las políticas establecidas.

Las condiciones necesarias para cumplir con este objetivo son:

- Personal capacitado
- Comunicación oportuna entre ventas, cobranzas y cliente
- Tener políticas de cobranza establecidas
- Disponibilidad de recursos humanos y físicos para la recuperación
- Contar con las garantías aprobadas.

**Alcance.**

Se aplica en todo CAVES SA EMA, para clientes de contado o crédito, sean personas naturales o jurídicas.

**MP: GESTIÓN DEL TALENTO HUMANO**

**CAPACITACIÓN AL PERSONAL.**

**Objetivos y Condiciones Necesarias:**

Detectar las necesidades de capacitación en los diferentes niveles de la organización, y desarrollar y ejecutar planes tendientes a cubrir estas necesidades, para adecuar al personal a las exigencias de su puesto.

Las condiciones necesarias para este proceso son:

- Disponer de recursos económicos
- Tener acceso a la infraestructura necesaria
- Conocer el mercado de proveedores
- Contar con personal idóneo para ejecutar el proceso
- Contar con el compromiso de la organización hacia la capacitación.

### 1.2.10 CARACTERIZACIÓN DEL DEPARTAMENTO DE TI

Para cubrir toda la geografía de la empresa en el área de sistemas se dispuso el departamento de de la siguiente manera.

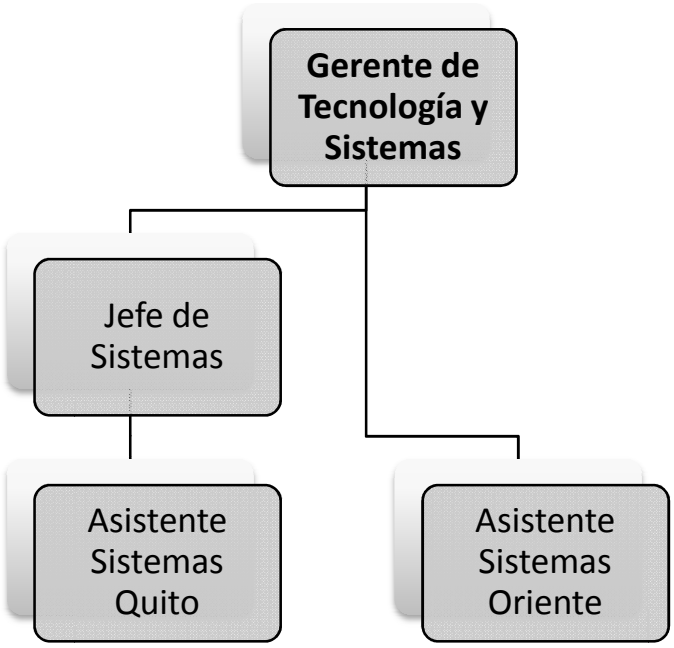



**Figura 1.11: Organigrama Departamento de Sistemas CAVES**

Dentro de los cargos que hay en el departamento se puede apreciar que también se han distribuido funciones por rol, por cada uno de los integrantes del departamento.

Se detallan a continuación algunos de los roles ejercidos por cada cargo detallado en el organigrama.

| Gerente de Tecnología y Sistemas | Jefe de Sistemas | Asistente Sistemas |
|---|---|---|
| • Investigación de nuevos productos<br>• Definición e Implementación de políticas de sistemas<br>• Administración SQL SERVER<br>• Administración de Redes y Comunicaciones<br>• Administración de Contratos<br>• Administración de Proveedores<br>• Administración Servidores<br>• Administración de Intranet<br>• Control de Licencias<br>• Seguridad ET (Estaciones de Trabajo) y Respaldos<br>• Administración de Aplicaciones<br>• Cotizaciones, inventarios de Equipos y Licencias<br>• Compras | • Administración Aplicativo ZEUS.<br>• Administración BDD SQL SERVER 20008<br>• Seguridad ET (Estaciones de Trabajo) y Respaldos.<br>• Administración Redes y Comunicaciones<br>• Administración de Aplicaciones<br>• Soporte Puntos de Servicios<br>• Compras.<br>• Soporte Sistema Control de Comidas SISCOM | • Soporte y Desarrollo Aplicativo Zeus.<br>• Soporte BDD SQL SERVER<br>• Soporte Aplicación SiSCom.<br>• Soporte Usuarios<br>• Soporte Software y Hardware.<br>• Soporte Redes - Comunicaciones<br>• Soporte Aplicaciones. |

**Figura 1.12: Descripción de Cargos Dpto. Sistemas CAVES**

### 1.2.11 INVENTARIO DE PROCESOS SOPORTADOS POR TI.

**Tabla 1.3: Inventario Procesos soportados por TI**

| Proceso | Descripción | Modificable | No Modificable |
|---|---|---|---|
| **Compras** | Proceso de Compras que inicia por la necesidad de compras por parte de las Operaciones del Oriente, o por la gestión misma del Dpto. de Compras. | **X** | |
| **Pedidos y Distribución** | Manejo de Inventario: Recepción y salida de los productos, Recepción de las Facturas de Proveedores | **X** | |
| **Financiero** | Soporta todos los procesos del departamento contable desde el cobro y pago de facturas, hasta la emisión de los reportes contables (Balances , Pérdidas y Ganancias) | **X** | |
| **Recursos Humanos** | Administra toda la gestión relacionada a la administración de los empleados, Datos de personal, Control de tiempos, Nómina. | **X** | |
| **Producción** | Elaboración de Menús, Planificación de la producción, Control de Costos. | **X** | |
| **Administración de Calidad y QHSE** | Evalúa el nivel de calidad de los productos y de los servicios | | **X** |

### 1.2.12 INVENTARIO DE PROCESOS CRÍTICOS DE LA EMPRESA Y SOPORTADOS POR TI

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada.

Para muchas organizaciones, la información y la tecnología que las soporta, representan los activos más valiosos de la empresa.

Por lo tanto, la administración debe valorar y comprender los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados.

A continuación se detalla los procesos críticos de la empresa, que son soportados por TI.

**Tabla 1.4: Procesos Críticos de la Empresa y soportados por TI**

| Proceso | Descripción | Justificación Criticidad |
|---|---|---|
| **Compras** | Proceso de Compras que inicia por la necesidad de compras por parte de las Operaciones del Oriente, o por la gestión misma del Dpto. de Compras. | Información Consolidad y en línea de todo el proceso de compras, que realizan todas las operaciones de la empresa. Información de Proveedores, productos, alternativas etc. |
| **Planificación** | Gestión de Inventario: Ingresos, Egresos, Traslados de productos, | Acceso al Inventario de cualquier Bodega, de las diferentes operaciones, con el objetivo de trasladar productos de un Punto a Otro, para optimizar el inventario que se maneja en cada bodega |
| **Planificación** | Desarrollo de Nuevos Puntos de Venta en el lugar y en Tiempo que el cliente Requiere | Montaje y Puesta en Marcha de Nuevos Puntos de Servicio en el Lugar Geográfico que el Cliente Requiera y bajo los requerimientos y Estándares del mismo, en un tiempo definido |
| **Recursos** | Gestión del Talento Humano, Reclutamiento, Enrolamiento, | Registro en Línea, de todas las novedades y necesidades de |

| | | |
|---|---|---|
| **Humanos** | Capacitación, Salida y Novedades . | puestos de Trabajo que se encuentran ubicados en las diferentes operaciones del Oriente. Acceso a información de empleados por parte de supervisores, y jefes departamentales. |
| **Producción** | Control de Consumos de Servicios por punto de Venta (Facturación) | Registro diario de todos los consumos de servicios y Productos por centros de costo, requisito indispensable para el proceso de facturación. |
| **Producción** | Elaboración de Menús, Planificación de la producción, Control de Costos. | Elaboración de recetas, con información real, de stocks y precio de productos, con el objetivo de costear platos, en la elaboración de Menús, ajustados a las especificaciones del Contrato. |
| **Administración de Calidad y QHSE** | Evalúa el nivel de calidad de los productos y de los servicios | Registro en Línea de las novedades que se pueden presentar, en lo que se refiere a la calidad de los servicios o productos, y además registrar, las observaciones o reclamos que realiza el cliente |

# CAPITULO 2

## 2.1 SELECCIÓN DE LOS PROCESOS A SER AUDITADOS.

### 2.1.1 FORMA DE SELECCIÓN 1

**Selección de los procesos mediante la relación de procesos críticos del negocio y las metas del negocio propuesto por cobit.**

#### 2.1.1.1 Procesos Críticos del Negocio vs del Metas del Negocio Cobit.

En base a la definición de la empresa estudiada en el Capitulo 1, en donde se identifica el ambiente interno y externo, y todos los procesos de la empresa, se logra realizar un inventario de Procesos críticos de la empresa y que son soportados por TI

Estos procesos críticos son relacionados con las Metas del Negocio Propuesto por Cobit, con el objetivo de seleccionar la Metas del Negocio en sus diferentes perspectivas, que se logren alinear con los procesos críticos del Negocio.

Esta relación entre los procesos Críticos de CAVES SA EMA , y las metas del Negocio Propuesto por Cobit, son representando en el siguiente gráfico.

**Tabla 2.1 : Procesos Claves del Negocio Alineados con la Metas del Negocio de Cobit**

| Metas del Negocio \ Procesos Clave del Negocio | | Compras Proveedores Productos | Gestión de Inventarios | Creación de Nuevos Puntos de Venta | Gestión del Talento Humano | Control Consumo Servicios y Productos Puntos de Venta | Planificación de Producción | Control de Calidad Productos y Servicios | PONDERACION |
|---|---|---|---|---|---|---|---|---|---|
| **Perspectiva Financiera** | 1. Proporcionar un buen retorno de Inversión de TI- permitiendo inversión en negocio | P | P | | | P | | | **3** |
| | 2. Gestionar los riesgos de TI que afecten a negocio | P | P | P | | P | | | **4** |
| | 3. Mejorar gobierno corporativo y transparencia | | | | | | | | **0** |
| **Perspectiva del Cliente** | 4. Mejorar la orientación y servicio al cliente | | | P | P | | P | P | **4** |
| | 5. Ofrecer Productos y servicios competitivos | P | | P | P | | | P | **4** |
| | 6. Establecer continuidad y disponibilidad del los servicios | P | P | P | | P | | | **4** |
| | 7. Crear agilidad en la respuesta a los cambios de los requerimientos del Negocio | P | P | P | P | | P | | **5** |
| | 8. Lograr optimización de costes de entrega de servicios | | | | | P | | | **1** |
| | 9. Obtener información fiable y útil para tomar decisiones estratégicas | P | P | | P | P | P | P | **6** |
| **Perspectiva Interna** | 10. Mejorar y mantener funcionalidad de proceso de negocio | P | P | | | P | | | **3** |
| | 11. Reducir el coste de los procesos | P | P | | | P | P | | **4** |
| | 12. Proporcionar cumplimiento con leyes externas, regulaciones y contratos | | | P | P | P | P | P | **5** |
| | 13. Proporcionar cumplimiento con políticas internas | P | P | | P | | | P | **4** |
| | 14. Gestionar cambios de negocio | P | P | P | P | | P | | **5** |
| | 15. Mejorar y mantener productividad operacional y de personal | | | | P | | | P | **2** |
| **Perspectiva de aprendizaje y crecimiento** | 16. Gestionar productos e innovación de negocio | P | P | P | | | P | P | **5** |
| | 17. Adquirir y mantener personal cualificado y motivado | | | | P | | | P | **2** |

Luego de realizar la asociación de las metas del negocio propuesto por Cobit con los procesos claves del Negocio, realizamos una ponderación, para obtener las principales metas del negocio que nos facilitaran la selección de los procesos cobit a auditar , las metas seleccionadas son las siguientes:

### 2.1.1.2 ENLACE ENTRE LAS METAS DEL NEGOCIO SELECCIONADAS Y LAS METAS DE TI

**Tabla 2.2: Enlace Metas del Negocio Cobit y Metas de TI**

| Metas del Negocio Seleccionadas | METAS DE TI | | | | | | | | Efectividad | Eficiencia | Confidencialidad | Integridad | Disponibilidad | Cumplimiento | Confiabilidad |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2. Gestionar los riesgos de TI que afecten a negocio | 2 | 14 | 17 | 18 | 19 | 20 | 21 | 22 | | | ✓ | ✓ | ✓ | | |
| 4. Mejorar la orientación y servicio al cliente | 3 | 23 | | | | | | | ✓ | | | | | | |
| 5. Ofrecer Productos y servicios competitivos | 5 | 24 | | | | | | | ✓ | ✓ | | | | | |
| 6. Establecer continuidad y disponibilidad del los servicios | 10 | 16 | 22 | 23 | | | | | ✓ | | | | ✓ | | |
| 7. Crear agilidad en la respuesta a los cambios de los requerimientos del Negocio | 1 | 5 | 25 | | | | | | ✓ | ✓ | | | | | |
| 9. Obtener información fiable y útil para tomar decisiones estratégicas | 2 | 4 | 12 | 20 | 26 | | | | | ✓ | | | | | |
| 11. Reducir el coste de los procesos | 7 | 8 | 13 | 15 | 24 | | | | | ✓ | | | | | |
| 12. Proporcionar cumplimiento con leyes externas, regulaciones y contratos | 2 | 19 | 20 | 21 | 22 | 26 | 27 | | | | ✓ | | | ✓ | |
| 13. Proporcionar cumplimiento con políticas internas | 2 | 13 | | | | | | | | | | | | | |
| 14. Gestionar cambios de negocio | 1 | 5 | 28 | | | | | | ✓ | ✓ | | | | | |
| 16. Gestionar productos e innovación de negocio | 5 | 25 | 28 | | | | | | ✓ | ✓ | | | | | |

### 2.1.1.3 MATRIZ DE PROCESOS DE TI A METAS DE TI.

Mediante el uso de la matriz de Procesos de TI con las Metas de TI, se realiza una ponderación para determinar los Procesos COBIT a Auditar en la Empresa.

## Tabla 2.3 Enlace de las Metas de TI Procesos de

| METAS DE TI => | | Responder a Requerimientos de negocio alineado con la estrategia del negocio | Responder a los requerimientos de gobierno en línea con la dirección del Consejo. | Garantizar la satisfacción del usuario final con las ofertas del servicio y los niveles del mismo. | Optimizar el uso de la Información | Generar agilidad en la TI. | Asegurar la satisfacción Mutua de relaciones con terceras partes | Asegurar la Transparencia y comprensión de Costos de TI | Asegurar el Uso Apropiado y desempeño de las soluciones de aplicación y tecnológica | Proteger y rendir cuentas por todos los activos de TI. | Reducir los defectos de la solución y entrega de servicio y reelaborar | Proteger el logro de los objetivos de TI. | Establecer claramente el impacto de negocio de los riesgos en los objetivos y recursos de TI. | Garantizar que la información crítica y confidencial se resguarda de quienes no deben tener acceso a la misma. | Garantizar que las transacciones de negocio y los intercambios de información automatizados son confiables. | Garantizar que los servicios y la infraestructura de TI pueden resistir y recuperarse a las fallas debidas a errores, ataques intencionales o desastres. | Garantizar el mínimo impacto de negocio en caso de una interrupción o un cambio en los servicios de TI. | Garantizar que los servicios de TI se encuentran disponibles según sea necesario. | Mejorar la Eficiencia de Costes de TI y sus contribuciones a la Renabilidad del Negocio | Entregar los proyectos a tiempo y dentro del presupuesto, cumpliendo con los estándares de calidad. | Mantener la integridad de la información e infraestructura de procesamiento | Asegurar que TI cumple con la legislación, regulación y contratos | Garantizar que la TI exhiba una calidad costo-eficaz de los servicios, una mejora continua y una buena disposición para cambios futuros. | EQUIVALENCIA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **PROCESOS DE TI** | **1** | **2** | **3** | **4** | **5** | **10** | **12** | **13** | **14** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** | **26** | **27** | **28** | |
| **PLANEACION Y ORGANIZACIÓN** | | | | | | | | | | | | | | | | | | | | | | | | |
| PO1 | Definición de un plan estratégico de TI | X | X | | | | | | | | | | | | | | | | | | | | | 100% |
| PO4 | Definición de los procesos, la organización y las relaciones de TI | X | X | | | X | | | | | | | | | | | | | | | | | | 100% |
| PO9 | Evaluación y gestión de riesgos | | | | | | | | | X | | X | X | | | | | | | | | | | 100% |
| PO10 | Gestión de proyectos | X | X | | | | | | | | | | | | | | | | | X | | | | 100% |
| **ADQUISICION E IMPLEMENTACION** | | | | | | | | | | | | | | | | | | | | | | | | |
| **ENTREGA Y SOPORTE** | | | | | | | | | | | | | | | | | | | | | | | | |
| DS2 | Gestión de los servicios prestados por terceros | | | X | | | X | X | | | | | | | | | | | | | | | | 100% |
| DS4 | Aseguramiento de la continuidad del servicio | | | | | | | | | | | | | | | X | X | X | | | | | | 100% |
| DS5 | Aseguramiento de la seguridad de los sistemas | X | | | | | | | | | | | | X | X | X | | | | | X | | | 100% |
| DS8 | Gestión de incidentes y de la mesa de soporte | | | X | | | | | X | | | | | | | | | X | | | | | | 100% |
| DS12 | Gestión del entorno físico | | | | | | | | | X | | | | X | | X | X | | | | | | | 100% |

### 2.1.1.4 PROCESOS TI SELECCIONADOS.

**Tabla 2.4: Procesos COBIT seleccionados mediante Forma 1**

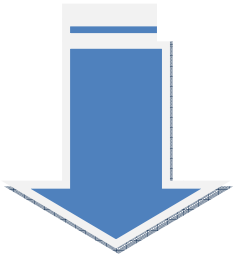
| METAS DE TI => | | EQUIVALENCIA |
|---|---|---|
| PROCESOS DE TI | | |
| **PLANEACION Y ORGANIZACIÓN** | | |
| PO1 | Definición de un plan estratégico de TI | 100% |
| PO4 | Definición de los procesos, la organización y las relaciones de TI | 100% |
| PO9 | Evaluación y gestión de riesgos | 100% |
| PO10 | Gestión de proyectos | 100% |
| **ADQUISICION E IMPLEMENTACION** | | |
| **ENTREGA Y SOPORTE** | | |
| DS2 | Gestión de los servicios prestados por terceros | 100% |
| DS4 | Aseguramiento de la continuidad del servicio | 100% |
| DS5 | Aseguramiento de la seguridad de los sistemas | 100% |
| DS8 | Gestión de incidentes y de la mesa de soporte | 100% |
| DS12 | Gestión del entorno físico | 100% |

Se toma los procesos con mayor ponderación, los mismos que estarían alineados con los Procesos Críticos del negocio.

A continuación se resumen toda la metodología de selección de procesos Forma1

**Gráfico : Resumen Procesos TI seleccionados.**


**Figura 2.1: Resumen Procesos COBIT seleccionados Forma 1**



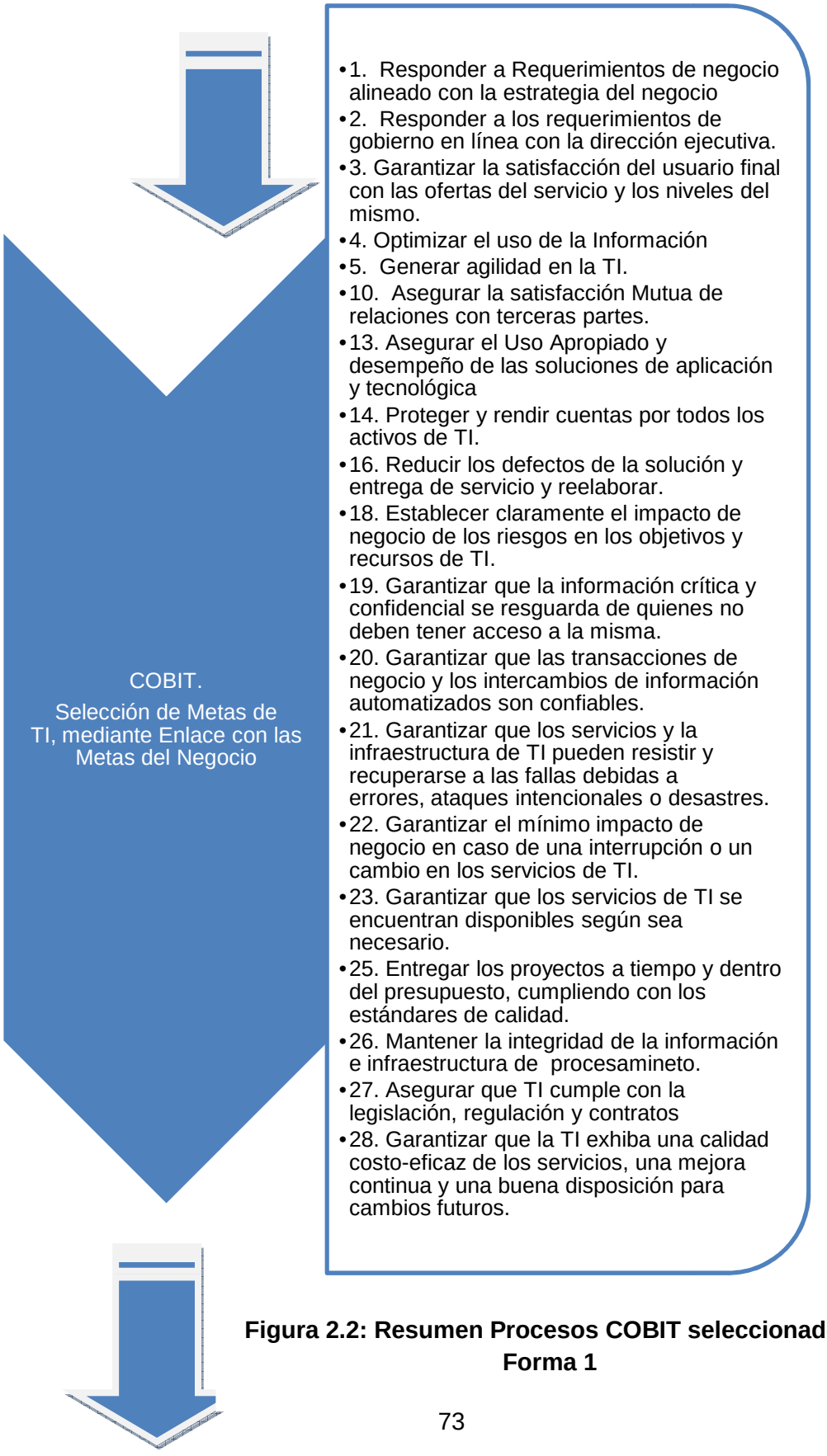



**Figura 2.2: Resumen Procesos COBIT seleccionados Forma 1**

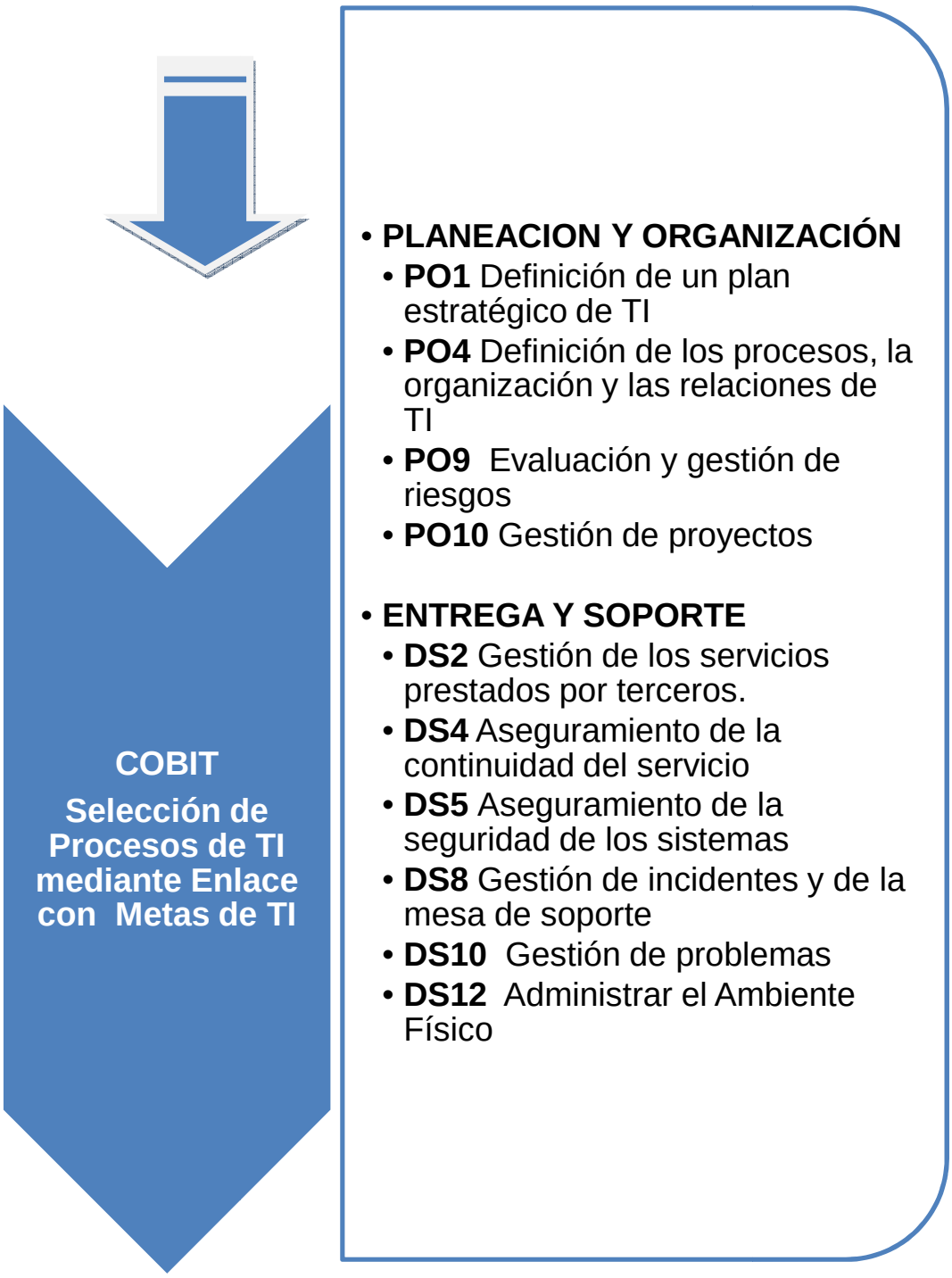



**Figura 2.3: Resumen Procesos COBIT seleccionados Forma 1**

### 2.1.2 FORMA DE SELECCIÓN 2

Para confirmar los procesos que serán auditadas, se usará solamente el Formulario de Identidad de un grupo de matrices o encuestas que propone ISACA en su libro “Cobit Implementation Tool Set”, está encuesta servirá para hacer un análisis de prioridades y de esta manera realizar una correcta selección de los procesos a Auditar.

#### 2.1.2.1 FORMULARIO DE ENTIDAD.

Ayuda a determinar la importancia, la funcionalidad y los controles que se están realizando en los procesos. La recopilación de esta información se enmarca en preguntas como las siguientes:

- **IMPORTANCIA**: La persona encuestada determinará, de acuerdo a sus roles dentro de la empresa, su nivel de trascendencia. Las posibles alternativas de respuesta son de mayor a menor los siguientes :
    - **Muy Importante**.
    - **Algo Importante**.
    - **No importante**.
    - **No está seguro**.
    - **No se aplica**.

- **DESEMPEÑO**: Busca que el encuestado identifique los niveles de resultados que se está obteniendo de las actividades realizadas para lo cual se tiene las siguientes opciones:
    - Excelente
    - Muy Bueno
    - Satisfactorio
    - Pobre

- **DIMENSIONADO FORMALMENTE**: Tiene dos opciones, la una que afirma la posibilidad planteada de que exista un parámetro de medición documentado que evalúe el desempeño individual. O la otra posibilidad, “no dimensionado”, cuando no ha existido una evaluación.

- El cuestionamiento de “Control Interno” se refiere a la documentación formal aprobada y difundida en la empresa, sobre las actividades realizadas y consultadas, para tal efecto el encuestado tiene las siguientes opciones a elegir.
    - Documentando.
    - No Documentado.
    - No está seguro.

## Tabla 2.5: Matriz de Entidad

**FORMULARIO DE ENTIDAD**

**DEPARTAMENTO:** **CARGO:**

| IMPORTANCIA | | | | | | DESEMPEÑO | | | | | | | Control Interno | | | WP. REF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Muy Importante | Algo Importante | No Importante | No se Aplica | | PROCESOS DE IT | Exelente | Muy Bueno | Satisfactorio | Pobre | No está Seguro | Dimensioado Formalmente | No se Aplica | Documentado | No Documentado | No esta Seguro | |
| | | | | | **PLANEACION Y ORGANIZACIÓN** | | | | | | | | | | | |
| | | | | PO1 | Definición de un plan estratégico de TI | | | | | | | | | | | |
| | | | | PO2 | Definición de la arquitectura de la información | | | | | | | | | | | |
| | | | | PO3 | Determinación de la dirección tecnológica | | | | | | | | | | | |
| | | | | PO4 | Definición de los procesos, la organización y las relaciones de TI | | | | | | | | | | | |
| | | | | PO5 | Gestión de la inversión en TI | | | | | | | | | | | |
| | | | | PO6 | Comunicación de los objetivos y la dirección de la Alta Gerencia | | | | | | | | | | | |
| | | | | PO7 | Gestión de recursos humanos de la TI | | | | | | | | | | | |
| | | | | PO8 | Gestión de la calidad | | | | | | | | | | | |
| | | | | PO9 | Evaluación y gestión de riesgos | | | | | | | | | | | |
| | | | | PO10 | Gestión de proyectos | | | | | | | | | | | |
| | | | | | **ADQUISICION E IMPLEMENTACION** | | | | | | | | | | | |
| | | | | AI1 | Identificación de soluciones automatizadas | | | | | | | | | | | |
| | | | | AI2 | Adquisición y mantenimiento del software de aplicación | | | | | | | | | | | |
| | | | | AI3 | Adquisición y mantenimiento de la infraestructura tecnológica | | | | | | | | | | | |
| | | | | AI4 | Habilitación de la operación y el uso | | | | | | | | | | | |
| | | | | AI5 | Abastecimiento de recursos de TI | | | | | | | | | | | |
| | | | | AI6 | Gestión de cambios | | | | | | | | | | | |
| | | | | AI7 | Instalación y acreditación de soluciones y cambios | | | | | | | | | | | |
| | | | | | **ENTREGA Y SOPORTE** | | | | | | | | | | | |
| | | | | DS1 | Definición de los niveles de servicio | | | | | | | | | | | |
| | | | | DS2 | Gestión de los servicios prestados por terceros | | | | | | | | | | | |
| | | | | DS3 | Gestión de la capacidad y del desempeño del sistema | | | | | | | | | | | |
| | | | | DS4 | Aseguramiento de la continuidad del servicio | | | | | | | | | | | |
| | | | | DS5 | Aseguramiento de la seguridad de los sistemas | | | | | | | | | | | |
| | | | | DS6 | Identificación y asignación de costos | | | | | | | | | | | |
| | | | | DS7 | Educación y capacitación de los usuarios | | | | | | | | | | | |
| | | | | DS8 | Gestión de incidentes y de la mesa de soporte | | | | | | | | | | | |
| | | | | DS9 | Gestión de la configuración | | | | | | | | | | | |
| | | | | DS10 | Gestión de problemas | | | | | | | | | | | |
| | | | | DS11 | Gestión de datos | | | | | | | | | | | |
| | | | | DS12 | Gestión del entorno físico | | | | | | | | | | | |
| | | | | DS13 | Gestión de operaciones | | | | | | | | | | | |
| | | | | | **MONITOREAR Y EVALUAR** | | | | | | | | | | | |
| | | | | M1 | Monitoreo y evaluación del desempeño de la TI | | | | | | | | | | | |
| | | | | M2 | Monitoreo y evaluación del control interno | | | | | | | | | | | |
| | | | | M3 | Aseguramiento del cumplimiento de reglamentaciones | | | | | | | | | | | |
| | | | | M4 | Asegurar el gobierno de la TI | | | | | | | | | | | |

### 2.1.2.2 SELECCIÓN DE LA MUESTRA.

Con el objetivo de encontrar la información más adecuada para el análisis y auditoría del Departamento de TI de la empresa CAVES SA EMA, se realizará la selección de un grupo de personas que proporcionen los datos que reflejan las vivencias del encuestado en sus áreas de trabajo.

Los grupos a ser considerados son de acuerdo a los que sugiere Cobit, siendo estos:

- **Parte Gerencial o Directorio:** Para conocer la opinión de cuáles son los temas de mayor interés para ellos, y que deben ser tomados en cuenta en la Auditoría.
- **Departamento de TI:** Tiene que ser evaluado, por lo tanto es importante la opinión de ellos en la prioridades de información recopilada.
- **Empleados:** Proporcionan las pautas para evaluar el funcionamiento de sistemas.

De cada grupo se ha calculado el 4% y se ha redondeado para determinar el número de participantes de la encuesta.

**Tabla 2.6: Muestra de Participantes Muestra**

| PARTICIPANTES | POBLACION | MUESTRA |
|---|---|---|
| **Directivos** | 6 | 1 |
| **Departamentos TI** | 4 | 1 |
| **Empleados** | 52 | 2 |

### 2.1.2.3 PROCESO DE RECOPILACIÓN DE INFORMACIÓN PARA LA SELECCIÓN DE PRIORIDADES Y RIESGOS.

Se realiza la selección de los procesos que las personas encuestadas consideraron importantes, en la Matriz de Diagnóstico.

Antes de iniciar con las encuestas, se ha preparado al personal y a los directivos para entender lo que significa aplicar la metodología COBIT, en su empresa, los beneficios que pueden obtener. Se elaboró una Síntesis Ejecutiva que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de COBIT.

Se Proporciona a los encuestados y sobre todo a la alta gerencia un entendimiento más detallado de los conceptos clave y principios de COBIT e identifica los cuatro dominios de COBIT y los correspondientes 34 procesos de TI.

### 2.1.2.4 TABULACION DE ENCUESTAS DE PROCESOS COBIT.

Se realiza la tabulación por cada uno de los dominios Cobit, para luego seleccionar los que resulten con mayor grado de importancia.

**DOMINIO PO: Planificación y Organización.**

Matriz de Encuesta: DIAGNOSTICO DE PRIORIDADES Y RIESGOS

Parámetro de Medición: Importancia.

**Tabla 2.7: Resumen Tabulación Muestra Dominio PO**

| RESUMEN POR MUESTRA | DIRECTIVOS | DEPARTAMENTO DE TI | EMPLEADO 1 | EMPLEADO 2 | PROMEDIO IMPORTANCIA |
|---|---|---|---|---|---|
| **PLANEACION Y ORGANIZACIÓN** | | | | | PROMEDIO |
| PO1 Definición de un plan estratégico de TI | 5 | 2 | 1 | 2 | 2,5 |
| PO2 Definición de la arquitectura de la información | 4 | 3 | 4 | 3 | 3,5 |
| PO3 Determinación de la dirección tecnológica | 4 | 2 | 1 | 2 | 2,25 |
| PO4 Definición de los procesos, la organización y las relaciones de TI | 4 | 2 | 5 | 2 | 3,25 |
| PO5 Gestión de la inversión en TI | 5 | 2 | 2 | 3 | 3 |
| PO6 Comunicación de los objetivos y la dirección de la Alta Gerencia | 5 | 2 | 1 | 3 | 2,75 |
| PO7 Gestión de recursos humanos de la TI | 3 | 3 | 2 | 2 | 2,5 |
| PO8 Gestión de la calidad | 4 | 4 | 4 | 3 | 3,75 |
| **PO9 Evaluación y gestión de riesgos** | 5 | 5 | 4 | 5 | **4,75** |
| **PO10 Gestión de proyectos** | 5 | 5 | 4 | 5 | **4,75** |

**Procesos Cobit que se Destacan:**

PO9 Evaluación y Gestión de Riesgos.

PO10 Gestión de Proyectos

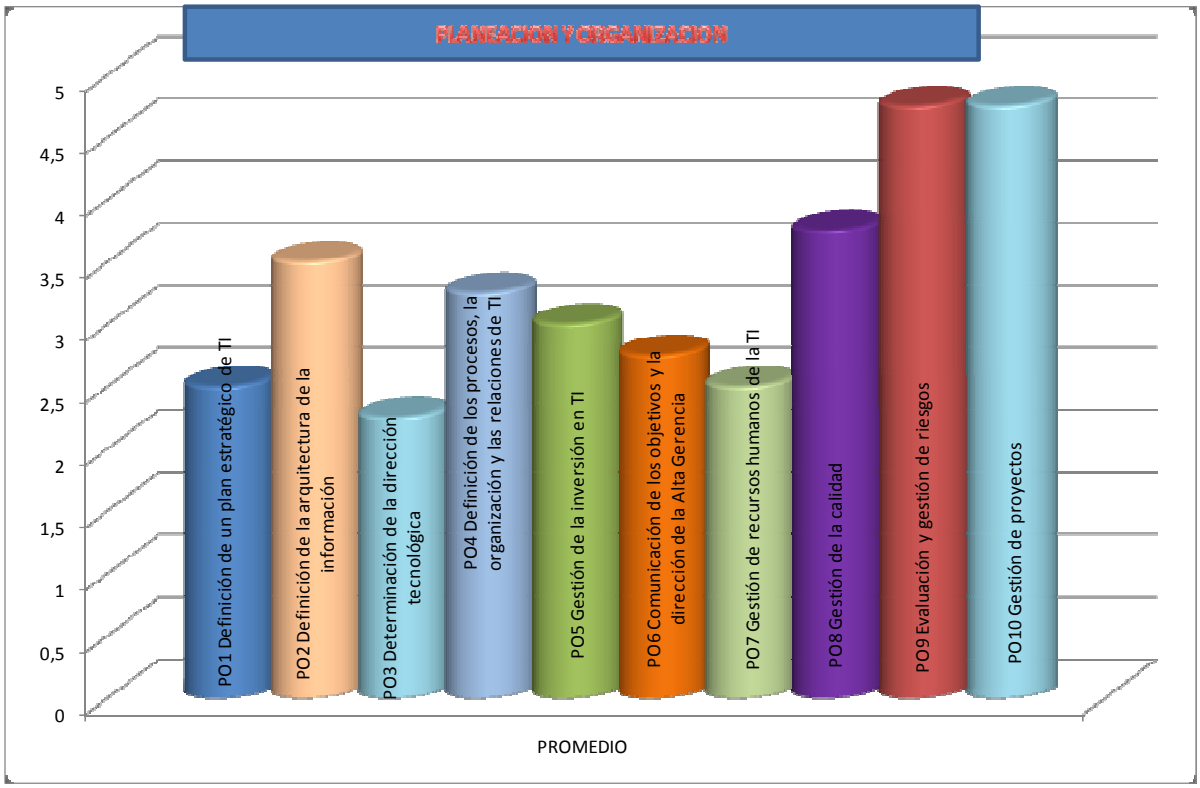



**Figura 2.4: Tabulación Muestra Dominio PO**

**DOMINIO AI: Adquisición e Implementación.**

Matriz de Encuesta: DIAGNOSTICO DE PRIORIDADES Y RIESGOS.

Parámetro de Medición: Importancia.

**Tabla 2.8: Resumen Tabulación Muestra Dominio AI**

| RESUMEN POR MUESTRA | DIRECTIVOS | DEPARTAMENTO DE TI | EMPLEADO 1 | EMPLEADO 2 | PROMEDIO IMPORTANCIA |
|---|---|---|---|---|---|
| **ADQUISICION E IMPLEMENTACION** | | | | | PROMEDIO |
| AI1 Identificación de soluciones automatizadas | 1 | 4 | 1 | 2 | 2 |
| AI2 Adquisición y mantenimiento del software de aplicación | 2 | 4 | 2 | 3 | 2,75 |
| **AI3 Adquisición y mantenimiento de la infraestructura tecnológica** | 3 | 4 | 5 | 4 | **4** |
| AI4 Habilitación de la operación y el uso | 3 | 2 | 2 | 2 | 2,25 |
| AI5 Abastecimiento de recursos de TI | 2 | 3 | 2 | 3 | 2,5 |
| AI6 Gestión de cambios | 3 | 3 | 3 | 2 | 2,75 |
| AI7 Instalación y acreditación de soluciones y cambios | 3 | 3 | 3 | 2 | 2,75 |

**Procesos Cobit que se Destacan:**

AI3 Adquisición y mantenimiento de la Infraestructura Tecnológica.

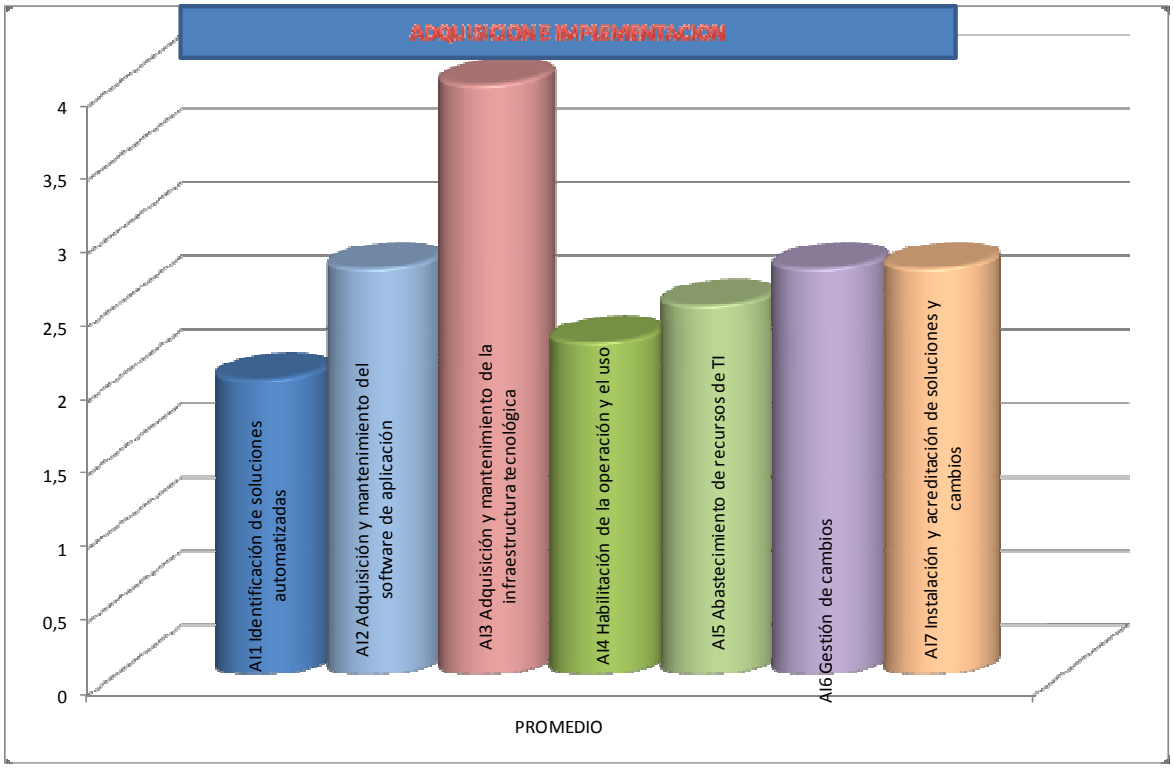



**Figura 2.5: Tabulación Muestra Dominio AI**

**DOMINIO DS: Entrega y Soporte.**

Matriz de Encuesta: DIAGNOSTICO DE PRIORIDADES Y RIESGOS.

Parámetro de Medición: Importancia.

**Tabla 2.9 : Resumen Tabulación Muestra Dominio DS**

| RESUMEN POR MUESTRA | DIRECTIVOS | DEPARTAMENTO DE TI | EMPLEADO 1 | EMPLEADO 2 | PROMEDIO IMPORTANCIA |
|---|---|---|---|---|---|
| **ENTREGA Y SOPORTE** | | | | | PROMEDIO |
| DS1 Definición de los niveles de servicio | 1 | 5 | 2 | 2 | 2,5 |
| **DS2 Gestión de los servicios prestados por terceros** | 4 | 5 | 3 | 3 | **3,75** |
| DS3 Gestión de la capacidad y del desempeño del sistema | 4 | 3 | 3 | 3 | 3,25 |
| DS4 Aseguramiento de la continuidad del servicio | 5 | 3 | 2 | 3 | 3,25 |
| **DS5 Aseguramiento de la seguridad de los sistemas** | 4 | 4 | 3 | 3 | **3,5** |
| DS6 Identificación y asignación de costos | 5 | 3 | 2 | 1 | 2,75 |
| **DS7 Educación y capacitación de los usuarios** | 3 | 3 | 4 | 5 | **3,75** |
| **DS8 Gestión de incidentes y de la mesa de soporte** | 4 | 4 | 5 | 4 | **4,25** |
| DS9 Gestión de la configuración | 1 | 4 | 2 | 1 | 2 |
| DS10 Gestión de problemas | 2 | 4 | 4 | 4 | 3,5 |
| DS11 Gestión de datos | 2 | 3 | 3 | 2 | 2,5 |
| DS12 Gestión del entorno físico | 3 | 3 | 3 | 2 | 2,75 |
| DS13 Gestión de operaciones | 3 | 3 | 2 | 2 | 2,5 |

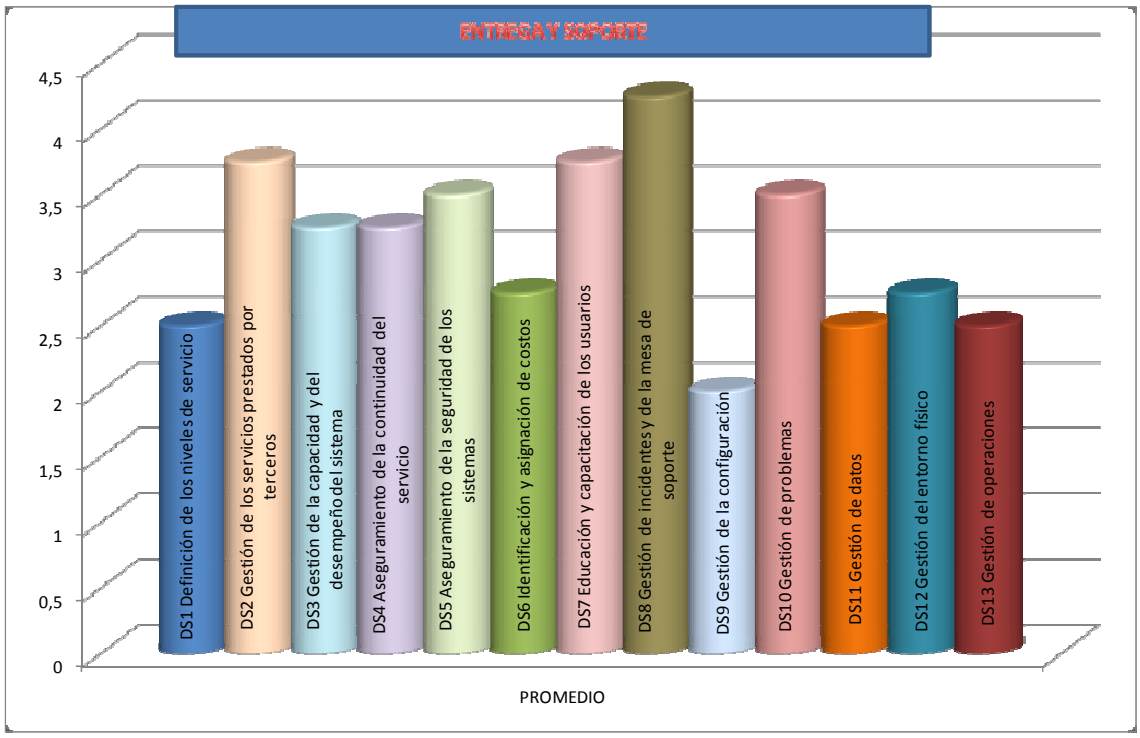
**Procesos Cobit que se Destacan:**

DS2 Gestión de los Servicios prestados por Terceros.

DS5 Aseguramiento de la seguridad de los sistemas

DS7 Educación y capacitación de los usuarios.

DS8 Gestión de incidentes y de la mesa de soporte



**DOMINIO M: MONITOREAR Y EVALUAR**

Matriz de Encuesta: DIAGNOSTICO DE PRIORIDADES Y RIESGOS.

Parámetro de Medición: IMPORTANCIA

**Tabla 2.10 : Resumen Tabulación Muestra Dominio M**

| RESUMEN POR MUESTRA | DIRECTIVOS | DEPARTAMENTO DE TI | EMPLEADO 1 | EMPLEADO 2 | PROMEDIO IMPORTANCIA |
|---|---|---|---|---|---|
| **MONITOREAR Y EVALUAR** | | | | | PROMEDIO |
| M1 Monitoreo y evaluación del desempeño de la TI | 3 | 3 | 3 | 2 | 2,75 |
| M2 Monitoreo y evaluación del control interno | 2 | 3 | 1 | 2 | 2 |
| M3 Aseguramiento del cumplimiento de reglamentaciones | 4 | 3 | 2 | 1 | 2,5 |
| M4 Asegurar el gobierno de la TI | 2 | 4 | 2 | 2 | 2,5 |

**Procesos Cobit que se Destacan.**

No se destacan proceso alguno.

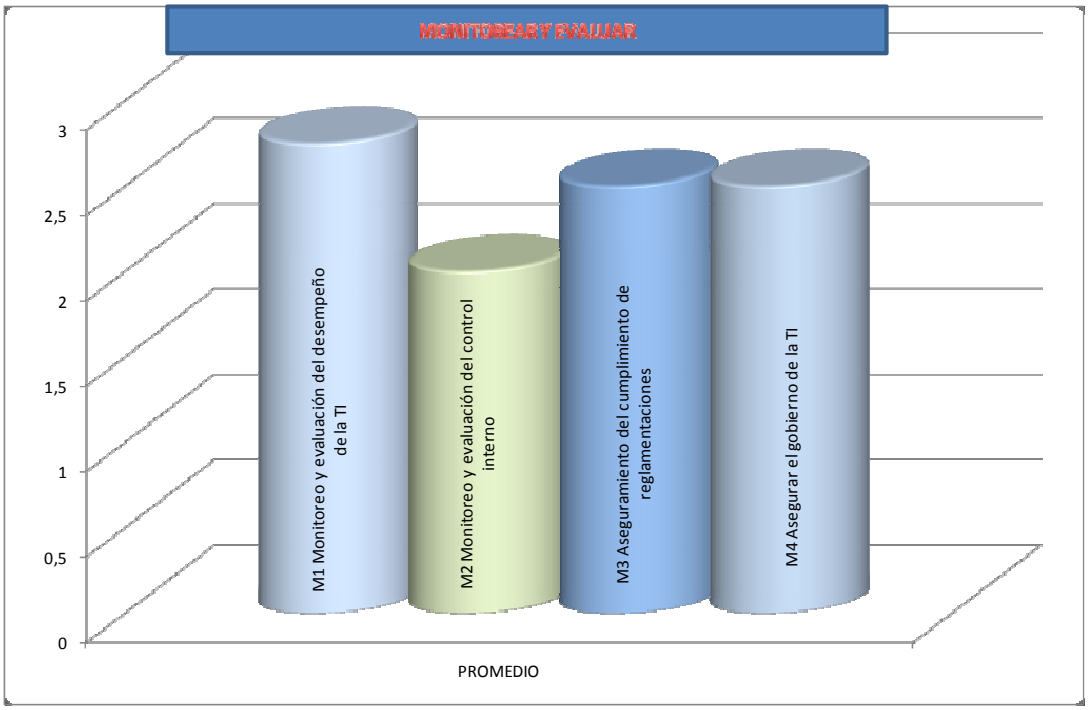



**Figura 2.7: Tabulación Muestra Dominio M**

## 2.1.2.5 RESUMEN DE LOS PROCESOS SELECCIONADOS FORMA 2

### Tabla 2.11: Resumen de los Procesos Seleccionados Forma 2

| | | | AREAS DE ENFOQUE DE GOBIERNO DE TI | | | | | RECURSOS DE TI DE COBIT | | | | CRITERIOS DE INFORMACION DE COBIT | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | IMPORTANCIA | ALINEACION ESTRATEGICA | ENTREGA DE VALOR | ADMINISTRACION DE | ADMINISTRACION DE | MEDICION DEL DESEMPEÑO | APLICACIÓN | INFORMACION | INFRAESTRUCTURA | PERSONAS | EFECTIVIDAD | EFICIENCIA | CONFIDENCIALIDAD | INTEGRIDAD | DISPONIBILIDAD | CUMPLIMIENTO | CONFIABILIDAD |
| **PLANEACION Y ORGANIZACIÓN** | | | | | | | | | | | | | | | | | | |
| PO9 | Evaluación y gestión de riesgos | A | P | | | | | | | | | S | S | P | P | P | S | S |
| PO10 | Gestión de proyectos | A | P | S | | | | | | | | P | P | | | | | |
| **ADQUISICION E IMPLEMENTACION** | | | | | | | | | | | | | | | | | | |
| AI3 | Adquisición y mantenimiento de la infraestructura tecnológica | B | | | | | | | | | | S | P | | S | S | | |
| **ENTREGA Y SOPORTE** | | | | | | | | | | | | | | | | | | |
| DS2 | Gestión de los servicios prestados por terceros | B | | P | S | P | S | | | | | P | P | S | S | S | S | S |
| DS5 | Aseguramiento de la seguridad de los sistemas | A | | | | P | | | | | | | | P | P | S | S | S |
| DS7 | Educación y capacitación de los usuarios | B | S | P | S | S | | | | | | P | S | | | | | |
| DS8 | Gestión de incidentes y de la mesa de soporte | B | | P | | | S | | | | | P | P | | | | | |

(P = Primario, S = Secundario)

## 2.1.3 SELECCIÓN DE PROCESOS COBIT PARA AUDITORIA.

Luego de realizar la selección de los procesos mediante dos formas, finalmente cruzamos los procesos y obtenemos los de mayor ponderación, para obtener finalmente los procesos a auditar.

**Tabla 2.12: Procesos a COBIT a Auditar**

| | | | | | | AREAS DE ENFOQUE DE GOBIERNO DE TI | | | | | | RECURSOS DE TI DE COBIT | | | | | CRITERIOS DE INFORMACION DE COBIT | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | IMPORTANCIA | PROCESOS TI FORMA 1 | MATRICES FORMA 2 | PONDERACION | ALINEACION ESTRATEGICA | ENTREGA DE VALOR | ADMINISTRACION DE | ADMINISTRACION DE | MEDICION DEL DESEMPEÑO | | APLICACIÓN | INFORMACION | INFRAESTRUCTURA | PERSONAS | | EFECTIVIDAD | EFICIENCIA | CONFIDENCIALIDAD | INTEGRIDAD | DISPONIBILIDAD | CUMPLIMIENTO | CONFIABILIDAD |
| **PLANEACION Y ORGANIZACIÓN** | | | | | | | | | | | | | | | | | | | | | | | |
| **PO9** | **Evaluación y gestión de riesgos** | A | X | X | 2 | P | | | | | | | | | | | S | S | P | P | P | S | S |
| **PO10** | **Gestión de proyectos** | A | X | X | 2 | P | S | | | | | | | | | | P | P | | | | | |
| **ENTREGA Y SOPORTE** | | | | | | | | | | | | | | | | | | | | | | | |
| **DS2** | **Gestión de los servicios prestados por terceros** | B | X | X | 2 | | P | S | P | S | | | | | | | P | P | S | S | S | S | S |
| **DS5** | **Aseguramiento de la seguridad de los sistemas** | A | X | X | 2 | | | | P | | | | | | | | | | P | P | S | S | S |
| **DS8** | **Gestión de incidentes y de la mesa de soporte** | B | X | X | 2 | | P | | | S | | | | | | | P | P | | | | | |

# CAPITULO 3

## 3.1 AUDITORIA

### 3.1.1 Estrategia de Auditoria

La presente Auditoria se realiza según los objetivos de control de CobiT mediante la obtención del entendimiento, evaluación de los controles existentes, realización de pruebas de cumplimiento y realización de pruebas sustantivas para finalmente decidir si se alcanza ó no el objetivo de control.

A continuación se resumen las fases a ejecutarse para conseguir los resultados esperados en la presente Auditoría

**Obtener entendimiento:**

Entrevistar al personal administrativo y de staff indicado para lograr la comprensión de:

- Los requerimientos del negocio y los riesgos asociados.
- La estructura organizacional.
- Los roles y responsabilidades.
- Las medidas de control establecidas.
- La actividad de reporte a la administración (estatus, desempeño, acciones).

Documentar los recursos de TI relacionados con el proceso que se ven especialmente afectados por el proceso bajo revisión. Confirmar el entendimiento del proceso bajo revisión, los Indicadores Clave de Desempeño (KPI) del proceso, las implicaciones de control, por ejemplo, mediante un seguimiento paso a paso del proceso.

**Evaluación de los controles**

Los pasos de auditoría a realizar en la evaluación de la eficacia de las medidas de control establecidas o el grado en el que se logra el objetivo de control. Básicamente, decidir qué se va a probar, si se va a probar y cómo se va a probar.

Evaluar la conveniencia de las medidas de control para el proceso bajo revisión mediante la consideración de los criterios identificados y las prácticas estándares de la industria, los Factores Críticos de Éxito (CSF) de las medidas de control y la aplicación del juicio profesional de auditor.

- Existen procesos documentados.
- Existen resultados apropiados.
- La responsabilidad y es clara y eficaz.
- Existen controles compensatorios en donde es necesario.


**Gráfico 3.1: Estrategia de Auditoría Para las Procesos Cobit Seleccionados.**

### 3.1.2 Proceso: PO9 - EVALUACIÓN Y GESTIÓN DE RIESGOS

### Dominio : PLANEACIÓN Y ORGANIZACIÓN

#### 3.1.2.1 INFORMACION

Se crea y mantiene un marco de administración de riesgos. Este marco documenta los niveles de riesgo de TI acordados, las estrategias de mitigación y los riesgos residuales. Se identifican, analizan y evalúan los posibles efectos sobre las metas la organización de los incidentes no planificados. Se adoptan estrategias de mitigación de riesgos a fin de minimizar el riesgo residual hasta un nivel aceptable. El resultado de la evaluación es comprensible para las partes interesadas y se detalla en términos financieros para que las partes interesadas puedan adecuar el riesgo a un nivel de tolerancia aceptable.

**Objetivo**

- Analizar y comunicar los riesgos de TI y su potencial impacto en los procesos y metas de negocio

**Enfocándose en:**

- El desarrollo de un marco de gestión de riesgos integrado en los marcos de gestión de negocio y de riesgos operacionales, en la evaluación de riesgos, en la mitigación de los mismos y en la comunicación de los riesgos residuales

**Es Posible Por:**

- El aseguramiento de que la gestión de riesgos está totalmente integrada en los procesos gerenciales, tanto interna como externamente, y que es aplicada sistemáticamente.
- La realización de evaluaciones de riesgo.
- La recomendación y comunicación de planes de acción para mitigar riesgos.

**Se mide con.**

- Porcentaje de objetivos críticos de TI cubiertos por la evaluación de riesgos.
- Porcentaje de riesgos críticos de TI identificados que cuentan con planes de acción desarrollados.
- Porcentaje de planes de acción de gestión de riesgos aprobados para su implementación.

### 3.1.2.2 OBTENCIÓN DEL ENTENDIMIENTO.

| Categoría | Descripción | Cumple | No Cumple |
|---|---|---|---|
| Entrevistas con: | Gerencia de TI | **SI** | |
| | Personal seleccionado de la Gerencia de TI | **SI** | |
| | Personal seleccionado de la administración de riesgos | | **NO** |
| | Usuarios clave de los servicios de TI | **SI** | |
| | | **Disponible** | |
| Revisión de documentación de: | Políticas y procedimientos relacionados con la evaluación de riesgos | **NO** | |
| | Documentos de evaluación de riesgos del negocio | **NO** | |
| | Documentos de evaluación de riesgos operativos | **SI** | |
| | Documentos de evaluación de riesgos de la Ti | **NO** | |
| | Detalles de la base sobre la cual se miden los riesgos y la exposición a los riesgos | **NO** | |
| | Archivos de personal para personal seleccionado de evaluación de riesgos | **SI** | |
| | Políticas de seguros que cubran el riesgo residual | **NO** | |
| | Resultados de la opinión de expertos | **NO** | |
| | Revisiones de grupos de colegas | **SI** | |
| | Ideas respecto de la base de datos de evaluación de riesgos | **SI** | |

### 3.1.2.3. EVALUACION OBJETIVOS DE CONTROL

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Planeación y Organización | | | |
| **PROCESO:** | | **PO9** Evaluación y Gestión de Riesgos | | | |
| **OBJETIVO DE CONTROL:** | | **P09.1** Alineación de la gestión de riesgos de negocios y de TI | | | |
| **DESCRIPCION:** | | Integrar los marcos de gobierno, gestión de riesgos y control de la TI con el marco de gestión de riesgos de la organización (empresarial). Incluir la alineación con la tolerancia al riesgo y con los niveles aceptables de riesgo de la empresa | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se integran los marcos de gobierno, gestión de riesgos y control de la TI con el marco de gestión de riesgos de la organización (empresarial)? | La empresa solo maneja un Sistema de Gestión de Riesgos para el Trabajador (SART), No se Evidencia un Marco de Gestión de riesgos de la Empresa | No | | Pobre |
| 2 | ¿Esto incluye la alineación con la tolerancia al riesgo y con los niveles aceptables de riesgo de la empresa? | No se Evidencia un Marco de Gestión de riesgos de la Empresa | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Planeación y Organización | | | |
| **PROCESO:** | | **PO9** Evaluación y Gestión de Riesgos | | | |
| **OBJETIVO DE CONTROL:** | | **P09.2** Establecimiento del contexto de los riesgos | | | |
| **DESCRIPCION:** | | Establecer un contexto para aplicar el marco de evaluación de riesgos a fin de garantizar los resultados adecuados. Incluir la determinación del contexto interno | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se establece un contexto para aplicar el marco de evaluación de riesgos a fin de garantizar los resultados adecuados? | No Existe Marco de Evaluación de Riesgos | No | | Pobre |
| 2 | ¿Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgo, las metas de la misma y los criterios con los cuales se evalúan los riesgos? | No Existe Marco de Evaluación de Riesgos | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Planeación y Organización | | | |
| **PROCESO:** | | **PO9** Evaluación y Gestión de Riesgos | | | |
| **OBJETIVO DE CONTROL:** | | **P09.3** Identificación de incidentes | | | |
| **DESCRIPCION:** | | Determinar la naturaleza de este impacto -positivo, negativo o ambos- y mantener esta información. Identificar todos los eventos (amenazas o vulnerabilidades) que tengan un potencial impacto en las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, operacionales, y de socios comerciales y recursos humanos | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se identifican todos los eventos (amenazas o vulnerabilidades) que tengan un potencial impacto en las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, operacionales, y de socios comerciales y recursos humanos? | Existe un Mapa de Riesgos Genéricos de la empresa, pero no incluyen los Riesgos Tecnológicos | NO | | Pobre |
| 2 | ¿Se determina la naturaleza de este impacto -positivo, negativo o ambos- y se mantiene esta información? | No esta Determinada la Naturaleza de Los Riesgos | NO | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Planeación y Organización | | | |
| **PROCESO:** | | **PO9** Evaluación y Gestión de Riesgos | | | |
| **OBJETIVO DE CONTROL:** | | **P09.3** Identificación de incidentes | | | |
| 3 | ¿Están identificados y clasificados los tipos de accesos?¿Y las razones que justifican el acceso? | Solo se limitan a definir Accesos No Autorizados | | SI | Satisfactorio |
| 4 | ¿Fueron identificados los riesgos de seguridad por contratos con terceros que trabajan "onsite" y se han puestos en práctica controles de seguridad apropiados? | No se han identificado los Riesgos para Terceros | NO | | Pobre |
| 5 | ¿Los análisis de riesgos son finalizados antes del comienzo del desarrollo de sistemas? | Los Riesgos No son Identificados antes del Desarrollo de Sistemas | NO | | Pobre |
| 6 | ¿Los requisitos de seguridad y los controles identificados reflejan el valor de los activos de información implicados y las consecuencias de una falla en la seguridad? | No se han identificado los Activos de Información, por consecuencia no Existe requisitos de seguridad identificados | NO | | Pobre |
| 7 | ¿Son incorporados requisitos de seguridad como parte de la declaración de requisitos del negocio para los nuevos sistemas o para mejoras a sistemas existentes? | No Existe Requisitos de Seguridad, para nuevos y sistemas existentes. | NO | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Planeación y Organización | | | |
| **PROCESO:** | | **PO9** Evaluación y Gestión de Riesgos | | | |
| **OBJETIVO DE CONTROL:** | | **P09.4** Evaluación de riesgos | | | |
| **DESCRIPCION:** | | Evalúar periódicamente la probabilidad y el impacto de todos los riesgos identificados empleando métodos cualitativos y cuantitativos. Determinar individualmente la probabilidad y el impacto asociados a los riesgos inherentes y residuales, tanto por su categoría como por su cartera | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se evalúa periódicamente la probabilidad y el impacto de todos los riesgos identificados empleando métodos cualitativos y cuantitativos? | No existe proceso de Evaluación de Riesgos, Una vez identificado el Riesgo se actua en forma Reactiva | NO | | Pobre |
| 2 | ¿Se determina individualmente la probabilidad y el impacto asociados a los riesgos inherentes y residuales, tanto por su categoría como por su cartera? | No se ha determinado la Probabilidad ni el impacto de los riesgos asociados. | NO | | Pobre |
| 3 | ¿Es obtenido el apoyo de especialista en seguridad de la información donde y cuando es apropiado? Un individuo específico puede ser identificado para coordinar conocimiento y experiencias internas para asegurar consistencia, y proporcionar ayuda en la toma de decisión sobre seguridad. | Existe Soporte de Especialistas en el Tema de Seguridad, pero solo cuando el Riesgo aparece | NO | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Planeación y Organización | | | |
| **PROCESO:** | | **PO9** Evaluación y Gestión de Riesgos | | | |
| **OBJETIVO DE CONTROL:** | | **P09.5** Respuesta al riesgo | | | |
| **DESCRIPCION:** | | Identificar a los propietarios de los riesgos y de los procesos afectados, desarrollar y mantener periódicamente una respuesta a los riesgos para garantizar que existen controles costo-eficaces y medidas de seguridad que mitigan la exposición a los riesgos. La respuesta al riesgo debe identificar estrategias para el riesgo como ser la evitación, reducción, participación o aceptación. Al desarrollar la respuesta, se deben considerar los costos y beneficios y se eligen las respuestas que limitan los riesgos a los niveles definidos de aceptación de riesgos | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se identifica a los propietarios de los riesgos y de los procesos afectados, y se desarrolla y mantiene periódicamente una respuesta a los riesgos para garantizar que existen controles costo-eficaces y medidas de seguridad que mitigan la exposición a los riesgos? | Se tienen identificado los Procesos que pueden ser afectados, pero no existe controles eficaces | NO | | Pobre |
| 2 | ¿La respuesta al riesgo identifica estrategias para el riesgo como ser la evitación, reducción, participación o aceptación? | No Existe un plan de Riesgos que permita identificar Estrategias de reducción de Riesgos | NO | | Pobre |
| 3 | Al desarrollar la respuesta, ¿se consideran los costos y beneficios y se eligen las respuestas que limitan los riesgos a los niveles definidos de aceptación de riesgos? | No Existe Niveles de Riesgo Definidos | NO | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Planeación y Organización | | | |
| **PROCESO:** | | **PO9** Evaluación y Gestión de Riesgos | | | |
| **OBJETIVO DE CONTROL:** | | **P09.6** Mantenimiento y monitoreo de un plan de acción de reducción de riesgos | | | |
| **DESCRIPCION:** | | Monitorear la ejecución de los planes, e informar de cualquier desviación a la Alta Gerencia. Priorizar y planificar las actividades de control a todos los niveles a fin de implementar las respuestas al riesgo identificadas como necesarias, incluyendo la identificación de costos, beneficios y responsabilidad de ejecución. Solicitar la aprobación de las acciones recomendadas y la aceptación de los riesgos residuales, y asegurar que las acciones tomadas pertenecen a los propietarios de los procesos afectados | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se priorizan y planifican las actividades de control a todos los niveles a fin de implementar las respuestas al riesgo identificadas como necesarias, incluyendo la identificación de costos, beneficios y responsabilidad de ejecución? | No Existe Plan de Acción de Reducción de Riesgos | NO | | Pobre |
| 2 | ¿Se solicita la aprobación de las acciones recomendadas y la aceptación de los riesgos residuales, y se asegura que las acciones tomadas pertenecen a los propietarios de los procesos afectados? | No Existe Plan de Acción de Reducción de Riesgos | NO | | Pobre |
| 3 | ¿Se monitorea la ejecución de los planes, y se informa de cualquier desviación a la Alta Gerencia? | No Existe Plan de Acción de Reducción de Riesgos | NO | | Pobre |

### 3.1.2.4. INDICADORES CLAVE DE DESEMPEÑO. KPI.

| RESPECTO A LAS ACTIVIDADES | | | |
|---|---|---|---|
| **METAS** | | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Asegurarse de que la administración de riesgos esté totalmente incluida en los procesos administrativos.<br><br>2.- Realizar evaluaciones de riesgo periódicas con los gerentes senior y con el personal clave. | **SE MIDE CON** | Porcentaje del presupuesto de TI gastado en actividades de administración de los riesgos (evaluación y mitigación). | **1%** |
| | | Frecuencia de la revisión del proceso de administración de riesgos de TI. | **Bajo** |
| | | Porcentaje de evaluaciones de riesgo autorizadas # de reportes de monitoreo de riesgos activados dentro de la frecuencia acordada. | **1%** |
| | | Porcentaje de eventos de TI identificados usados en evaluaciones de riesgo. | **1%** |
| | | Porcentaje de planes de acción de administración de riesgos aprobados para su implantación. | **1%** |
| *LOS INDICADORES CLAVE DE DESEMPEÑO DIRIGEN LAS METAS DE LOS PROCESOS* | | | |

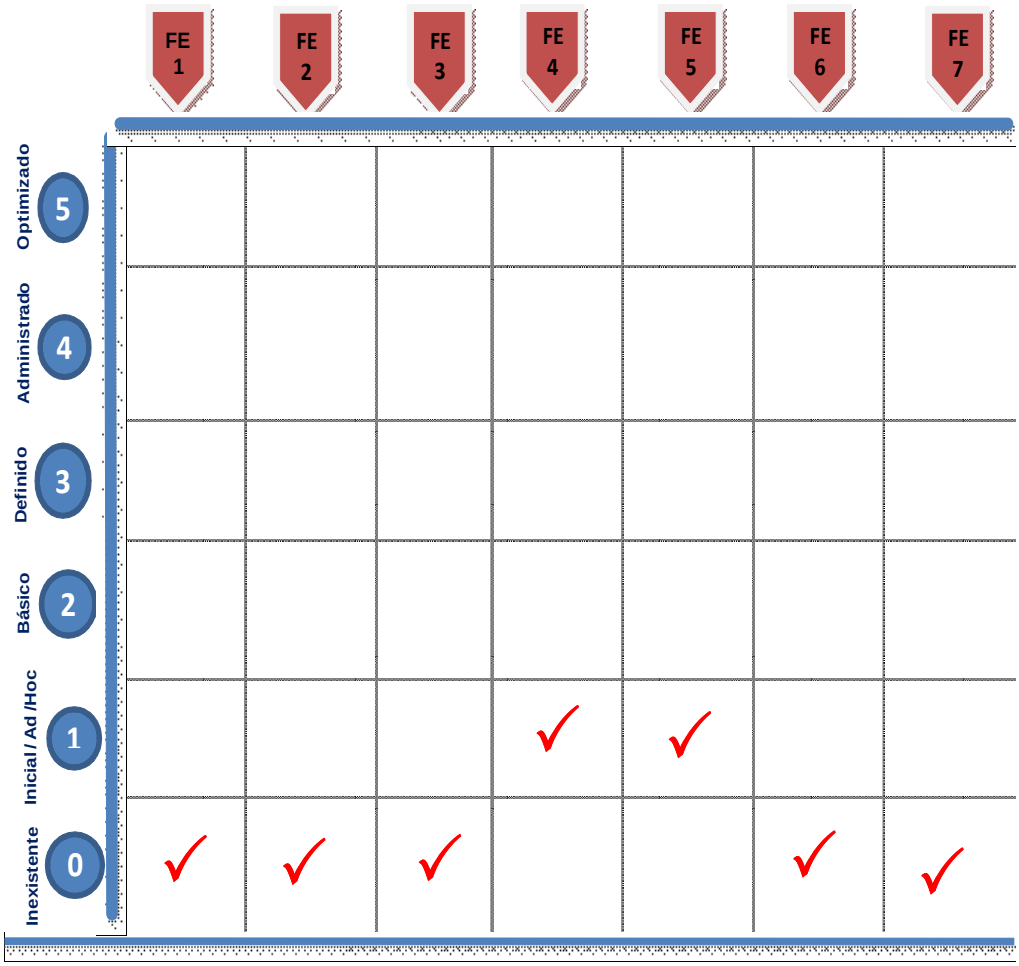
| RESPECTO A LOS PROCESOS | | | |
|---|---|---|---|
| **METAS** | **SE MIDE CON** | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Establecer y reducir la posibilidad y el impacto de los riesgos de TI.<br><br>2.- Establecer planes de acción rentables para los riesgos críticos de TI. | | Porcentaje de eventos críticos de TI identificados que han sido evaluados. | **5%** |
| | | Número de riesgos de TI recientemente identificados (comparados con el ejercicio previo). | **10%** |
| | | Número de incidentes significativos causados por riesgos no identificados por el proceso de evaluación de riesgos. | **1** |
| | | Porcentaje de riesgos críticos de TI identificados con un plan de acción elaborado. | **5%** |
| | | | |
| *LOS INDICADORES CLAVE DE PROCESOS DIRIGEN LAS METAS DE TI* | | | |

| RESPECTO A TI | | | |
|---|---|---|---|
| **METAS** | **SE MIDE CON** | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Proteger el logro de los objetivos de TI.<br><br>2.- Establecer claridad sobre el impacto en el negocio de los riesgos a los objetivos y recursos de TI.<br><br>3.- Responder por y proteger todos activos de TI. | | Porcentaje de objetivos críticos de TI cubiertos por la evaluación de riesgos. | **1%** |
| | | Porcentaje de evaluaciones de riesgos de TI integrados en el enfoque de evaluación de riesgos de TI. | **1%** |
| | | | |

### 3.1.2.5. FACTORES DE EVALUACIÓN DE LA MADUREZ.

| | |
|---|---|
|  | ***Políticas, Estándares y Procedimientos.*** |
|  | ***Responsabilidad, Rendición de Cuentas y Atención al Cliente.*** |
|  | ***Herramientas y Automatización.*** |
|  | ***Conciencia y Comunicación.*** |
|  | ***Habilidades y Experiencia.*** |
|  | ***Establecimiento y Medición de Metas.*** |
|  | ***Control Interno.*** |

### 3.1.2.6. NIVEL DE MADUREZ PROCESO PO9.



**NIVEL DE MADUREZ DETERMINADO**

**PO9 Evaluación y Gestión de Riesgos**: **Inexistente** 


**3.1.2.7. RAZONES PARA DICHA EVALUACIÓN:**

La evaluación del riesgo para los procesos y las decisiones del negocio no ocurre. La organización no considera los impactos de negocio asociados con vulnerabilidades de la seguridad y con incertidumbres de proyectos de desarrollo. La administración de riesgos no es identificada como relevante para la entrega de servicios o adquisición de soluciones de TI.

La debilidad en la evaluación y administración de los riesgos de TI se encuentra en la falta de definición formal de los roles y responsabilidades.

Además, no existe una metodología formal para la identificación de riesgos tecnológicos por lo que su administración se realiza de manera intuitiva y se podría dar una evaluación incompleta de los mismos

**Nivel Deseable.** 


Nivel Básico

## 3.1.3 Proceso: PO10 - GESTION DE PROYECTOS.

## Dominio : PLANEACIÓN Y ORGANIZACIÓN

### 3.1.3.1 INFORMACION

Se establece un marco de administración de proyectos y programas para administrar todos los proyectos de TI. Este marco garantiza que todos los proyectos son coordinados y priorizados correctamente. El marco incluye: un plan maestro, asignación de recursos, definición de entregables, aprobación de los usuarios, entregas en etapas, aseguramiento de la calidad, un plan de pruebas formal, y pruebas y revisiones post implantación luego de la instalación para garantizar la administración de riesgos del proyecto y la entrega de valor al negocio. Este enfoque minimiza el riesgo de los costos inesperados y las cancelaciones de proyectos, mejora la participación y la comunicación con el negocio y los usuarios finales, garantiza el valor y la calidad de los entregables del proyecto y maximiza el aporte a los programas de inversión posibilitados por la TI.

**Objetivo**

- Entregar los resultados de los proyectos dentro de los plazos, presupuestos y calidad acordados

**Enfocándose en:**

- La definición de un programa y un enfoque de gestión de proyectos que se aplique a los proyectos de TI, lo cual posibilita la participación y el monitoreo de los riegos y el avance del proyecto de las partes interesadas

**Es Posible Por:**

- La definición y cumplimiento de los programas, marcos de trabajo y enfoques de los proyectos.
- La publicación de directrices de gestión de proyectos.
- El realizar una planificación de proyectos para cada proyecto detallado en la cartera.

**Se mide con.**

- Porcentaje de proyectos que cumplen las expectativas de las partes interesadas (en tiempo, dentro del presupuesto, y que cumplen con los requerimientos ponderados por su importancia).
- Porcentaje de proyectos que reciben revisiones de post–implantación.
- Porcentaje de proyectos que siguen los estándares y prácticas de la gestión de proyectos.

### 3.1.3.2 OBTENCIÓN DEL ENTENDIMIENTO

| Categoría | Descripción | Cumple | No Cumple |
|---|---|---|---|
| Entrevistas con: | Gerente de Calidad | X | |
| | gerente/Coordinador de la Calidad de Proyectos | | X |
| | Propietarios/Patrocinadores del Proyecto | | X |
| | Lider del Equipo del Proyecto | X | |
| | Coordinador de Aseguramiento de la Calidad | X | |
| | Oficial de Seguridad | | X |
| | Miembros del comité de planificador/conductor de TI. | | X |
| | Gerencia de TI | X | |

| Categoría | Descripción | Cumple | No Cumple |
|---|---|---|---|
| | | Disponible | |
| Revisión de documentación de: | Políticas y procedimientos relacionados con el marco referencial de administración de proyectos | SI | |
| | Políticas y procedimientos relacionados con la metodología de administración de proyectos | NO | |
| | Políticas y procedimientos relacionados con los planes de aseguramiento de la calidad | SI | |
| | Políticas y procedimientos relacionados con los métodos de aseguramiento de la calidad | NO | |
| | Plan Maestro del Proyecto de Software (Software Project Master Plan - SPMP)) | NO | |
| | Plan de Aseguramiento de la Calidad del Software (Software Quality Assurance Plan - SQAP)) | NO | |
| | Informes de situación del proyecto | SI | |
| | Informes de situación y actas de las reuniones del comité de planificación. | SI | |
| | Informes de calidad del proyecto | NO | |

### 3.1.3.3 EVALUACION OBJETIVOS DE CONTROL

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.1** Marco de gestión de programas | | | |
| **DESCRIPCION:** | | Mantener el programa de proyectos relacionados con la cartera de programas de inversión posibilitados por la TI, mediante la identificación, definición, evaluación, priorización, selección, iniciación, gestión y control de los proyectos. Garantizar que los proyectos apoyan los objetivos del programa. Coordinar las actividades e interdependencias de múltiples proyectos, gestionar la contribución a los resultados esperados de todos los proyectos dentro del programa, y resolver los conflictos de requerimientos de recursos | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se mantiene el programa de proyectos relacionados con la cartera de programas de inversión posibilitados por la TI, mediante la identificación, definición, evaluación, priorización, selección, iniciación, gestión y control de los proyectos? | Existe una Planificación Anual de los Posibles Proyectos a Desarrollarse, quedando la selección de Prioridades por parte de las Gerencias de la empresa, en el Comité Anual de Operaciones | No | | Pobre |
| 2 | ¿Se garantiza que los proyectos apoyan los objetivos del programa? | Los Requerimientos de Proyectos son solicitados a TI, por parte de las Gerencia de cada unos de los Departamentos, y luego con la selección de los Proyectos de Desarrollarse se envidencia que los Proyectos apoyan a los Objetivos del Programa. | No | | Pobre |
| 3 | ¿Se coordinan las actividades e interdependencias de múltiples proyectos, se gestiona la contribución a los resultados esperados de todos los proyectos dentro del programa, y se resuelven los conflictos de requerimientos de recursos? | La interdependencia de los Multiples Proyectos son Gestionados por la Gerencia de TI que se encarga de resolver los posibles conflictos de requerimientos de recursos | No | | Pobre |

| | | | | |
|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.2** Marco de gestión de proyectos | | |
| **DESCRIPCION:** | | Los marcos y las metodologías de apoyo deben estar integrados con la cartera de gestión empresarial y los procesos de gestión de programas. Establecer y mantener un marco de gestión de proyectos que defina el alcance y los límites de los proyectos de gestión, así como las metodologías a ser adoptadas y aplicadas a cada proyecto emprendido. Las metodologías deben cubrir, como mínimo, el inicio, la planificación, la ejecución, el control y el cierre de las etapas del proyecto, así como puntos de control y aprobaciones | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** / **ANEXO** | |
| 1 | ¿Está establecido y se mantiene un marco de gestión de proyectos que defina el alcance y los límites de los proyectos de gestión, así como las metodologías a ser adoptadas y aplicadas a cada proyecto emprendido? | No Existe un Marco de Gestión de Proyectos, solo se evidencia que Los Proyectos son desarrollados con una Metodología apropiada | No | Pobre |
| 2 | ¿Las metodologías cubren, como mínimo, el inicio, la planificación, la ejecución, el control y el cierre de las etapas del proyecto, así como puntos de control y aprobaciones? | La Metodología utilizada cumple con los requerimientos básicos en el desarrollo de un Proyecto | No | Pobre |
| 3 | ¿Los marcos y las metodologías de apoyo están integrados con la cartera de gestión empresarial y los procesos de gestión de programas? | No Existe un Marco de Gestión de Proyectos. | No | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.3** Enfoque de la gestión de proyectos | | | |
| **DESCRIPCION:** | | Garantizar que todos los proyectos de TI tienen patrocinadores con la suficiente autoridad como para ser propietarios de la ejecución del proyecto dentro de una programa de estrategia global. Establecer un enfoque para la gestión de proyectos acorde al tamaño, complejidad y los requerimientos regulatorios de cada proyecto. La estructura de gobierno de los proyectos debe incluir los roles, las responsabilidades, y la rendición de cuentas por parte del patrocinador del programa, los patrocinadores del proyecto, el comité de dirección, el oficial y el encargado del proyecto, así como los mecanismos a través de los cuales se pueden satisfacer estas responsabilidades (como ser el informar acerca de las revisiones de cada etapa) | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Está establecido un enfoque para la gestión de proyectos acorde al tamaño, complejidad y los requerimientos regulatorios de cada proyecto? | No está establecido un enfoque para la Gestión. Todos los Proyectos son coordinados por el Gerente de Sistemas, el único parámetro que distingue un proyecto de Otro, es la importancia y Prioridades | No | | Pobre |
| 2 | ¿La estructura de gobierno de los proyectos incluye los roles, las responsabilidades, y la rendición de cuentas por parte del patrocinador del programa, los patrocinadores del proyecto, el comité de dirección, el oficial y el encargado del proyecto, así como los mecanismos a través de los cuales se pueden satisfacer estas responsabilidades (como ser el informar acerca de las revisiones de cada etapa)? | La Estructura de Gobierno de los Proyectos, solo incluye roles y responsabilidades por fases. | No | | Pobre |
| 3 | ¿Se garantiza que todos los proyectos de TI tienen patrocinadores con la suficiente autoridad como para ser propietarios de la ejecución del proyecto dentro de una programa de estrategia global? | Los Patrocinadores de los Proyectos de TI , son los Gerentes de Areas, con autoridad para la Ejecución de los Proyectos, pero la última aprobación lo realiza el Comité de Operaciones | No | | Satisfactorio |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.4** Compromiso de las partes interesadas | | | |
| | **DESCRIPCION:** | Obtener la participación y el compromiso de las partes interesadas afectadas para la definición y ejecución del proyecto dentro del contexto de un programa de inversión global posibilitado por la TI | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se obtiene la participación y el compromiso de las partes interesadas afectadas para la definición y ejecución del proyecto dentro del contexto de un programa de inversión global posibilitado por la TI? | Si Existe la participación y el Compromiso de las partes interesadas | No | | Satisfactorio |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.5** Declaración de alcance del proyecto | | | |
| **DESCRIPCION:** | | Definir y documentar la naturaleza y el alcance del proyecto para ratificar y desarrollar una comprensión común entre las partes interesadas acerca su alcance y cómo el mismo se relaciona con otros proyectos dentro del programa de inversión global posibilitado por la TI. Aprobar formalmente esta definición por parte de los patrocinadores del programa y del proyecto antes de iniciar el mismo | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se define y documenta la naturaleza y el alcance del proyecto para ratificar y desarrollar una comprensión común entre las partes interesadas acerca su alcance y cómo el mismo se relaciona con otros proyectos dentro del programa de inversión global posibilitado por la TI? | Todos los Proyectos Incluyen Objetivos y alcance, es compredido entre las partes interesadas, ya que durante la elaboración toman participación | No | | Satifactorio |
| 2 | ¿Se aprueba formalmente esta definición por parte de los patrocinadores del programa y del proyecto antes de iniciar el mismo? | Los Proyectos son revisados por los Patrocinadores y aprobados por el Comité de Operaciones | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.6** Comienzo de la fases del proyecto | | | |
| **DESCRIPCION:** | | La aprobación de las etapas subsiguientes debe basarse en la revisión y aceptación de los entregables de la etapa anterior, y la aprobación para actualizar el caso de negocio se obtiene en la siguiente revisión significativa del programa. La aprobación de las etapas iniciales deben basarse en las decisiones de gobernabilidad del programa. Asegurar que el inicio de las etapas principales del proyecto son aprobados formalmente y comunicados a todas las partes interesadas. Si las etapas del proyecto se solapan, se debe establecer una instancia de aprobación para que los patrocinadores del programa y del proyecto den su autorización para continuar con el proyecto | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se asegura que el inicio de las etapas principales del proyecto es aprobado formalmente y comunicado a todas las partes interesadas? | El Proyecto es Aprobado en su totalidad no por etapas, y es comunicado a las partes interesadas | No | | Pobre |
| 2 | ¿La aprobación de las etapa inicial se basa en las decisiones de gobernabilidad del programa? | El Proyecto es Aprobado en su totalidad no por etapas. | No | | Pobre |
| 3 | ¿La aprobación de las etapas subsiguientes se basa en la revisión y aceptación de los entregables de la etapa anterior, y la aprobación para actualizar el caso de negocio se obtiene en la siguiente revisión significativa del programa? | El Proyecto es Aprobado en su totalidad, no por Etapas | No | | Pobre |
| 4 | Si las etapas del proyecto se solapan, ¿se establece una instancia de aprobación para que los patrocinadores del programa y del proyecto den su autorización para continuar con el proyecto? | El Proyecto es evaluado solo cuando finaliza o cuando se cancela el mismo | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.7** Plan Integrado del Proyecto | | | |
| **DESCRIPCION:** | | Establecer un plan de proyecto formal, aprobado e integrado (que abarque los recursos de negocio y de información de sistemas) a fin de guiar la ejecución y el control del proyecto a lo largo de todo su ciclo de vida. Comprender y documentar las actividades e interdependencias de múltiples proyectos dentro de un programa. Mantener el plan del proyecto a lo largo de todo su ciclo de vida. Aprobar el plan del proyecto y los cambios del mismo en línea con el programa y con el marco de gobierno del proyecto | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Está establecido un plan de proyecto formal, aprobado e integrado (que abarque los recursos de negocio y de información de sistemas) a fin de guiar la ejecución y el control del proyecto a lo largo de todo su ciclo de vida? | No Existe un Plan de Proyecto Formal, que guie durante la ejecución del Control del Proyecto | No | | Pobre |
| 2 | ¿Se comprenden y documentan las actividades e interdependencias de múltiples proyectos dentro de un programa? | No Existe un Programa que abarque Multiples Proyectos, Los Proyectos se administran independientemente. | No | | Pobre |
| 3 | ¿Se mantiene el plan del proyecto a lo largo de todo su ciclo de vida? | El Proyecto no se mantiene fijo durante el ciclo de Vida, siempre tiene sus ajustes. | No | | Pobre |
| 4 | ¿Se aprueba el plan del proyecto y los cambios del mismo en línea con el programa y con el marco de gobierno del proyecto? | No Existe un marco de Gobierno del Proyecto | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.8** Recursos del proyecto | | | |
| **DESCRIPCION:** | | Planificar y gestionar el abastecimiento de los productos y servicios necesarios para cada proyecto a fin de alcanzar los objetivos del mismo, empleando las prácticas de abastecimiento de la organización. Definir responsabilidades, relaciones, autoridades y criterios de desempeño para los miembros del equipo del proyecto, y proporcionar la base para procurar y asignar personal calificado y/o proveedores para el proyecto especificado | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se definen responsabilidades, relaciones, autoridades y criterios de desempeño para los miembros del equipo del proyecto, y esto proporciona la base para procurar y asignar personal calificado y/o proveedores para el proyecto especificado? | Solo existe definidos los responsables por etapas del Proyecto | No | | Pobre |
| 2 | ¿Se planifica y gestiona el abastecimiento de los productos y servicios necesarios para cada proyecto a fin de alcanzar los objetivos del mismo, empleando las prácticas de abastecimiento de la organización? | No Existe Planificación para el abastecimiento de los productos | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.9** Administrar los Riesgos del proyecto | | | |
| | **DESCRIPCION:** | Eliminar o minimizar los riesgos específicos asociados con los proyectos individuales a través de un proceso sistemático de planificación, identificación, análisis, respuesta, monitoreo y control de las áreas o eventos que puedan ocasionar cambios no deseados. Establecer y registrar de forma centralizada los entregables del proyecto y los riesgos a los que se enfrenta el proceso de gestión del mismo | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se eliminan o minimizan los riesgos específicos asociados con los proyectos individuales a través de un proceso sistemático de planificación, identificación, análisis, respuesta, monitoreo y control de las áreas o eventos que puedan ocasionar cambios no deseados? | En los Proyectos no están identificados los Riesgos asociados | No | | Pobre |
| 2 | ¿Se establecen y registran de forma centralizada los entregables del proyecto y los riesgos a los que se enfrenta el proceso de gestión del mismo? | No Existe definición de Riesgos Asociados a los Proyectos | No | | Pobre |

| | | | | |
|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.10** Plan de Calidad del Proyecto | | |
| **DESCRIPCION:** | | Debe existir un plan de gestión de la calidad que describa el sistema de calidad del proyecto y cómo se implementa el mismo. Este plan se debe revisar y acordar formalmente entre todas las partes involucradas y es luego incorporado al plan de proyecto integrado | | |

| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
|---|---|---|---|---|---|
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Existe un plan de gestión de la calidad que describe el sistema de calidad del proyecto y cómo se implementa el mismo? | No Existe un Plan de Gestión de Calidad | No | | Pobre |
| 2 | ¿Este plan se revisa y acuerda formalmente entre todas las partes involucradas y es luego incorporado al plan de proyecto integrado? | No Existe un Plan de Gestión de Calidad | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.11** Control de Cambios del proyecto | | | |
| **DESCRIPCION:** | | Establecer un sistema de control de cambios para cada proyecto a fin de que todos los cambios a las referencias del proyecto (por ej. costos, calendarios, alcances y calidad) sean revisados, aprobados e incorporados al plan de proyecto integrado de forma adecuada, en línea con el programa y con el marco de gobierno del proyecto | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Está establecido un sistema de control de cambios para cada proyecto a fin de que todos los cambios a las referencias del proyecto (por ej. costos, calendarios, alcances y calidad) sean revisados, aprobados e incorporados al plan de proyecto integrado de forma adecuada, en línea con el programa y con el marco de gobierno del proyecto? | No Existe un Sistema de Control de Cambios para el Desarrollo de Proyectos | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.12** Planeación del Proyecto y Métodos de Aseguramiento | | | |
| **DESCRIPCION:** | | Exigir tareas de aseguramiento para apoyar la acreditación de sistemas nuevos o modificados identificados durante la planificación del proyecto, e incluir a las mismas en el plan de proyecto integrado. Estas tareas deben garantizar que los controles internos y las funciones de seguridad satisfacen los requerimientos definidos | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se exigen tareas de aseguramiento para apoyar la acreditación de sistemas nuevos o modificados identificados durante la planificación del proyecto, y se incluye a las mismas en el plan de proyecto integrado? | No Existe tareas de aseguramiento para apoyar la acreditación de sistemas nuevos | No | | Pobre |
| 2 | ¿Estas tareas garantizan que los controles internos y las funciones de seguridad satisfacen los requerimientos definidos? | No Existe tareas de aseguramiento para apoyar la acreditación de sistemas nuevos | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.13** Medición de Desempeño, Reporte y Monitoreo del Proyecto | | | |
| **DESCRIPCION:** | | Medir el desempeño del proyecto en relación a los criterios clave del proyecto (por ej. alcance, calendarios, calidad, costos y riesgos). Recomendar, implementar y monitorear las acciones remediales que sean necesarias, en línea con el programa y con el marco de gobierno del proyecto. Informar a las partes interesadas clave acerca de los resultados. Identificar y evalúar todas las desviaciones del plan en relación a su impacto en el proyecto y en el programa global | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se mide el desempeño del proyecto en relación a los criterios clave del proyecto (por ej. alcance, calendarios, calidad, costos y riesgos)? | No Existe un Sistema de Medición de Desempeño, y Monitoreo del Proyecto | No | | Pobre |
| 2 | ¿Se identifican y evalúan todas las desviaciones del plan en relación a su impacto en el proyecto y en el programa global? | No Existe un Sistema de Monitoreo del Proyecto | No | | Pobre |
| 3 | ¿Se informa a las partes interesadas clave acerca de los resultados? | No Existe un Sistema de Monitoreo del Proyecto | No | | Pobre |
| 4 | ¿Se recomiendan, implementan y monitorean las acciones remediales que sean necesarias, en línea con el programa y con el marco de gobierno del proyecto? | No Existe un Sistema de Monitoreo del Proyecto | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **PO** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **PO10** Gestión de proyectos | | | |
| **OBJETIVO DE CONTROL:** | | **DS.10.14** Cierre del Proyecto | | | |
| **DESCRIPCION:** | | Exigir que al final de cada proyecto las partes interesadas determinen si el proyecto entregó los resultados y beneficios planificados. Identificar y comunicar cualquier actividad necesaria aún pendiente para alcanzar los resultados planificados del proyecto y los beneficios del programa. Identificar y documentar las lecciones aprendidas a fin de ser usadas en futuros proyectos y programas | | | |

| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
|---|---|---|---|---|---|
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se exige que al final de cada proyecto las partes interesadas determinen si el proyecto entregó los resultados y beneficios planificados? | Existe un Documento de Acta / Entrega Recepción de los Proyectos, y aceptación por parte de los Patrocinadores | No | | Pobre |
| 2 | ¿Se identifica y comunica cualquier actividad necesaria aún pendiente para alcanzar los resultados planificados del proyecto y los beneficios del programa? | No Se Identifican Actividades pendientes | No | | Pobre |
| 3 | ¿Se identifican y documentan las lecciones aprendidas a fin de ser usadas en futuros proyectos y programas? | No se Documentan las lecciones aprendidas en el Desarrollo de los Proyectos | No | | Pobre |

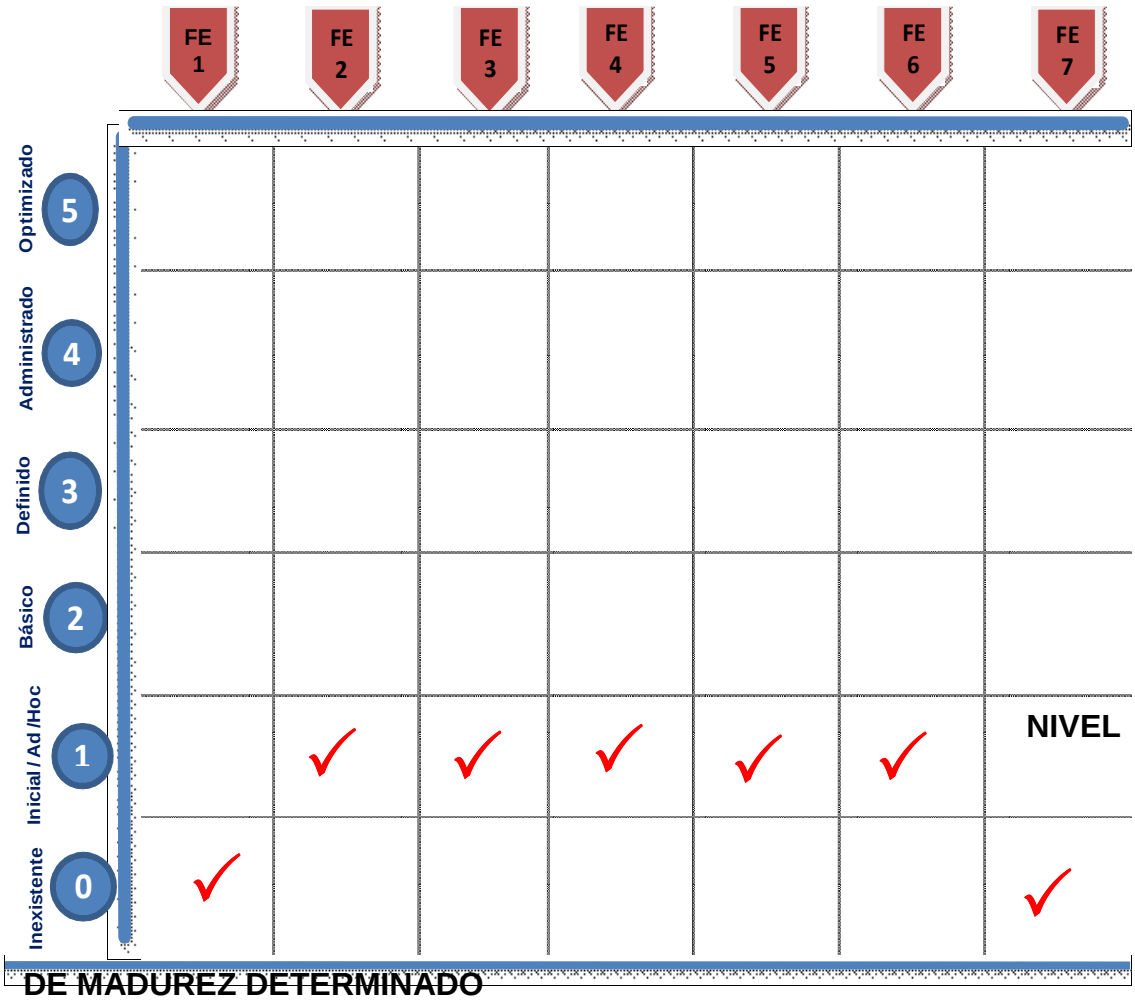
### 3.1.3. 4. INDICADORES CLAVE DE DESEMPEÑO. KPI.

| RESPECTO A LAS ACTIVIDADES | | | |
|---|---|---|---|
| **METAS** | | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Definir e implantar marcos de trabajo y enfoque para programas y proyectos.<br><br>2.- Emitir directrices administrativas para proyectos.<br><br>3.- Realizar planeación para cada proyecto contenido en el portafolio de proyectos. | **SE MIDE CON** | Indicadores clave de desempeño. | **0%** |
| | | Porcentaje de proyectos que siguen los estándares y las prácticas administrativas de proyectos. | **0%** |
| | | Porcentaje de gerentes de proyecto certificados o entrenados. | **1%** |
| | | Porcentaje de proyectos que reciben revisiones post-implantación. | **0%** |
| | | Porcentaje de interesados que participan en proyectos (índice de involucramiento). | **25%** |
| *LOS INDICADORES CLAVE DE DESEMPEÑO DIRIGEN LAS METAS DE LOS PROCESOS* | | | |

| RESPECTO A LOS PROCESOS | | | |
|---|---|---|---|
| **METAS** | | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Establecer mecanismos de seguimiento y de control de costos/tiempos para los proyectos. | **SE MIDE CON** | Porcentaje de proyectos a tiempo y dentro del presupuesto. | **10%** |
| 2.- Proporcionar transparencia del estatus de los proyectos.<br>3.- Tomar decisiones oportunas en la administración de proyectos en los puntos críticos. | | Porcentaje de proyectos que satisfacen las expectativas de los interesados. | **60%** |
| | | | |
| *LOS INDICADORES CLAVE DE PROCESOS DIRIGEN LAS METAS DE TI* | | | |

| RESPECTO A TI | | | |
|---|---|---|---|
| **METAS** | **SE MIDE CON** | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Responder a los requisitos del negocio de acuerdo a la estrategia del negocio.<br>2.- Entregar proyectos a tiempo y dentro del presupuesto, satisfaciendo estándares de calidad.<br>3.- Responder a los requerimientos de gobierno de acuerdo a la dirección establecida por el consejo directivo. | | Porcentaje de proyectos que satisfacen las expectativas de los interesados (a tiempo, dentro del presupuesto y que satisfacen los requerimientos – ponderados por importancia). | **50%** |

### 3.1.3.5. NIVEL DE MADUREZ PROCESO PO10.




**DE MADUREZ DETERMINADO**

**PO10 Gestión de proyectos: Inicial**

### 3.1.3.6 RAZONES PARA DICHA EVALUACIÓN:

El uso de técnicas y métodos de administración de proyectos dentro de la TI es una decisión que se deja a los administradores individuales de TI. Hay una falta general de compromiso por parte de la gerencia respecto a la propiedad de los proyectos y la administración de los mismos. Las decisiones críticas de administración de proyectos se hacen sin administración de usuarios o la contribución del cliente. Hay poca o ninguna participación de los clientes y los usuarios en la definición de los proyectos de TI. No hay una organización clara dentro de la TI para la administración de los proyectos. Los roles y responsabilidades de la administración de proyectos no están definidos. Los proyectos, cronogramas e hitos de los mismos están pobremente definidos. El tiempo y los gastos del personal del proyecto no son seguidos y comparados con los presupuestos.

**Nivel Deseable.**


Salto Importante a la Formalidad : **Nivel Básico**

### 3.1.4 Auditoria Proceso: DS2 - GESTIÓN DE LOS SERVICIOS PRESTADOS POR TERCEROS

**Dominio : ENTREGA Y SOPORTE**

#### 3..1.4.1 INFORMACION

Es necesario un proceso de administración eficaz para verificar que los servicios provistos por terceros (proveedores y socios) cumplen con los requerimientos de negocio. Este proceso se logra al definir claramente los roles, las responsabilidades y las expectativas en los acuerdos para terceros, revisando y supervisando además dichos acuerdos para verificar su eficacia y cumplimiento. Una administración eficaz de los servicios provistos por terceros minimiza los riesgos de negocio asociados con el incumplimiento de los proveedores.

**Objetivo**

- Proporcionar servicios tercerizados satisfactorios al tiempo que se mantiene la transparencia respecto a los beneficios, costos y riesgos

**Enfocándose en:**

- El establecimiento de relaciones y responsabilidades bilaterales con terceros proveedores de servicios calificados y en el monitoreo de la entrega del servicio para verificar y garantizar el respeto de los acuerdos.

**Es Posible Por:**

- - La identificación y categorización de los servicios prestados por los proveedores.
- - La identificación y mitigación del riesgo asociado a los proveedores.
- - El monitoreo y medición del desempeño del proveedor.

**Se mide con.**

- Número de quejas de los usuarios debido a los servicios contratados.
- Porcentaje de proveedores principales que cumplen con requerimientos y niveles de servicio claramente definidos.
- Porcentaje de proveedores principales que son monitoreados.

### 3.1.4.2. OBTENCION DEL ENTENDIMIENTO

| Categoría | Descripción | Cumple | No Cumple |
|---|---|---|---|
| Entrevistas con: | Director de TI (CIO) | | X |
| | Dirección de TI de TI. | X | |
| | Administrador del nivel de servicio/contrato de servicios de la información | | X |
| | Administrador de operaciones de la Dirección de TI | | X |
| | Oficial de Seguridad de la Dirección de TI | | X |
| | | Disponible | |
| Revisión de documentación de: | Políticas generales para la organización asociadas con los servicios adquiridos y en particular, con las relaciones con proveedores como terceras partes | NO | |
| | Políticas y procedimientos de la Dirección de TI asociadas con: relaciones con terceras partes, procedimientos de selección de proveedores, contenido del control de dichas relaciones, seguridad lógica y física, mantenimiento de la calidad por parte de los proveedores, planificación de contingencias y fuentes externas | NO | |
| | Una lista de todas las relaciones actuales con terceras partes y de los contratos reales asociados con ellas | SI | |
| | El reporte del nivel de servicio relacionado con las relaciones y servicios proporcionados por terceras partes | NO | |
| | Las actas de las reuniones en las que se discuten la revisión de los contratos, la evaluación del desempeño y la administración de las relaciones | SI | |
| | Los acuerdos de confidencialidad para todas las relaciones con terceras partes | SI | |
| | Las listas de seguridad de acceso con los perfiles y recursos disponibles para los proveedores | NO | |

### 3.1.4.3. EVALUACION OBJETIVOS DE CONTROL

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entrega y Soporte | | | |
| **PROCESO:** | | **DS2** Administrar los Servicios de Terceros | | | |
| **OBJETIVO DE CONTROL:** | | **DS2.1** Identificación de relaciones con proveedores | | | |
| **DESCRIPCION:** | | Identificar y categorizar todos los servicios de los proveedores de acuerdo al tipo de proveedor y a su importancia y criticidad. Mantener una documentación formal de las relaciones técnicas y organizacionales, que cubre los roles y las responsabilidades, las metas, los entregables esperados y las credenciales de los representantes de estos proveedores | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se identifican y categorizan todos los servicios de los proveedores de acuerdo al tipo de proveedor y a su importancia y criticidad? | Existe una Clasificación de Proveedores por el Tipo de Servicio, pero no por su importancia y Criticidad | No | | Satisfactorio |
| 2 | ¿Se mantiene una documentación formal de las relaciones técnicas y organizacionales, que cubre los roles y las responsabilidades, las metas, los entregables esperados y las credenciales de los representantes de estos proveedores? | El único documento formal que se evidencia son los contratos de servicios en donde solo e detalla las relaciones técnicas pero no detalla roles responsabilidades etc. | Si | | Satisfactorio |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entrega y Soporte | | | |
| **PROCESO:** | | **DS2** Administrar los Servicios de Terceros | | | |
| **OBJETIVO DE CONTROL:** | | **DS2.2** Gestión de relaciones con proveedores | | | |
| **DESCRIPCION:** | | Los propietarios de las relaciones deben ser el enlace entre el cliente y el proveedor cuando existen desacuerdos y deben garantizar la calidad de la relación basándose en la confianza y la transparencia (por ejemplo a través de acuerdos de nivel de servicio). Formalizar el proceso de gestión de relaciones para cada proveedor | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se formaliza el proceso de gestión de relaciones para cada proveedor? | La Gestión de relación con el Proveedor se evidencia en el Contrato Firmado | No | | Pobre |
| 2 | ¿Los propietarios de las relaciones hacen de enlace entre el cliente y el proveedor cuando existen desacuerdos y garantizan la calidad de la relación basándose en la confianza y la transparencia (por ejemplo a través de acuerdos de nivel de servicio)? | No se evidencia Acuerdos de Nivel de Servicio | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entrega y Soporte | | | |
| **PROCESO:** | | **DS2** Administrar los Servicios de Terceros | | | |
| **OBJETIVO DE CONTROL:** | | **DS2.3** Administración de riesgos de proveedores | | | |
| | **DESCRIPCION:** | La gestión de riesgos debe considerar a su vez acuerdos de confidencialidad (NDAs), contratos de depósitos en garantía, viabilidad de la continuidad del proveedor, proveedores alternativos, sanciones y recompensas, etc. Asegurar que los contratos se ajustan a los estándares generales de negocios de acuerdo a los requisitos legales y regulatorios. Identificar y mitigar continuamente los riesgos relativos a la capacidad del proveedor de mantener una entrega de servicios eficaz de forma segura y eficiente | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se identifican y mitigan continuamente los riesgos relativos a la capacidad del proveedor de mantener una entrega de servicios eficaz de forma segura y eficiente? | No se evidencia los riesgos relativos a la capacidad del Proveedor | No | | Pobre |
| 2 | ¿Se asegura que los contratos se ajustan a los estándares generales de negocios de acuerdo a los requisitos legales y regulatorios? | Si, los Contratos se ajustan a los estandares y requerimientos del negocio | Si | | Satisfactorio |
| 3 | ¿La gestión de riesgos considera a su vez acuerdos de confidencialidad (NDAs), contratos de depósitos en garantía, viabilidad de la continuidad del proveedor, proveedores alternativos, sanciones y recompensas, etc.? | Se Evidencia en los contratos existe acuerdo de confidencialidad de la información, pero no existe información de proveedores alternativos, sanciones , recompensas etc. | Si | | Pobre |
| 4 | ¿Cuando la organización tiene fuera de si el manejo y control de todos o algunos de sus sistemas de información, redes y/o ambientes de escritorio, los requisitos de seguridad son tratados en el contrato con terceros? | Los Controles de los sistemas de información son tratados en su totalidad por la empresa | No | | Satisfactorio |
| 5 | ¿El contrato establece como se deben cumplir los requisitos legales, cómo es mantenida y testada la seguridad de los activos de la organización, el derecho de intervención, y aspectos de seguridad física? | En el contrato no se evidencia el tema de seguridad de los activos de la organización, y aspectos de seguridad física. | No | | Pobre |
| 6 | ¿Existe un contrato formal que contenga, o refiera, todos los requisitos de seguridad para asegurar conformidad con las políticas y los estándares de seguridad de la organización? | En el contrato no se evidencia el tema de seguridad de los activos de la organización, y aspectos de seguridad física. | No | | Pobre |
| 7 | ¿Se mantienen contactos apropiados con autoridades de la aplicación de ley, cuerpos reguladores, proveedores de servicios de información y operadores de la telecomunicación para asegurarse que, ante el acontecimiento de un incidente la seguridad, serán tomadas la acciones apropiada y se obtendrá consejo rápidamente? | En el contrato no se evidencia el tema de seguridad de los activos de la organización, y aspectos de seguridad física. | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entrega y Soporte | | | |
| **PROCESO:** | | **DS2** Administrar los Servicios de Terceros | | | |
| **OBJETIVO DE CONTROL:** | | **DS2.4** Monitoreo del desempeño de los proveedores | | | |
| | **DESCRIPCION:** | Debe existir un proceso establecido para monitorear la entrega de servicios a fin de garantizar que el proveedor satisface los requerimientos de negocio actuales y cumple con los acuerdos del contrato y del nivel de servicio, y que el desempeño es competitivo respecto a proveedores alternativos y a las condiciones de mercado | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Existe un proceso establecido para monitorear la entrega de servicios a fin de garantizar que el proveedor satisface los requerimientos de negocio actuales y cumple con los acuerdos del contrato y del nivel de servicio, y que el desempeño es competitivo respecto a proveedores alternativos y a las condiciones de mercado? | No existe Procedimiento o Proceso establecido, se evidencia solamente Actas entregas / Recepción de los trabajos realizados por los Proveedores | No | | Pobre |

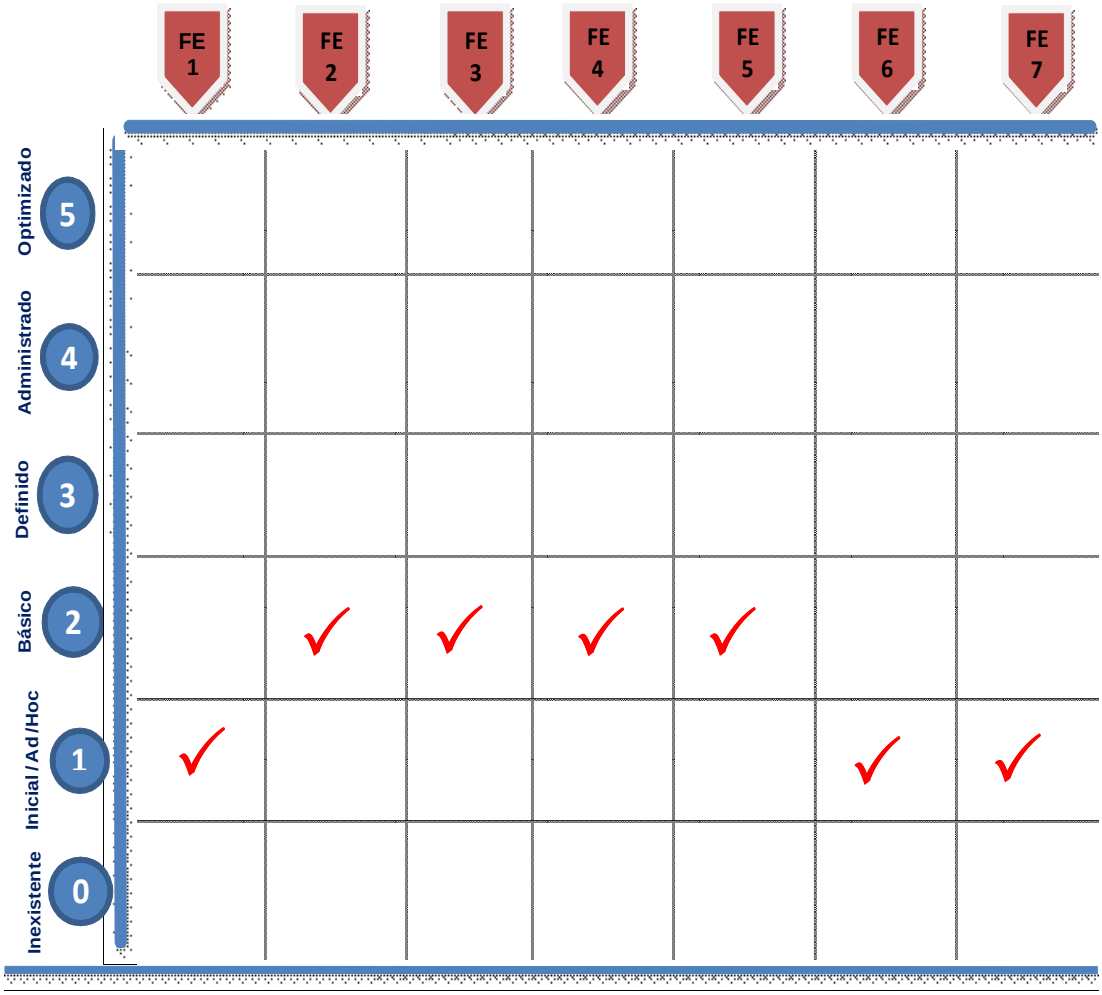
### 3.1.4.4. INDICADORES CLAVE DE DESEMPEÑO. KPI.

| RESPECTO A LAS ACTIVIDADES | | | |
|---|---|---|---|
| **METAS** | | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Identificación y categorización de los servicios del proveedor.<br><br>2.- Identificación y mitigación de riesgos del proveedor.<br><br>3.- Monitoreo y medición del desempeño del proveedor. | **SE MIDE CON** | Porcentaje de los principales proveedores sujetos a una clara definición de requerimientos y niveles de servicio. | **50%** |
| | | Porcentaje de los principales proveedores sujetos a monitoreo. | **40%** |
| | | Nivel de satisfacción del negocio con comunicación efectiva por parte del proveedor. | **MEDIO** |
| | | Nivel de satisfacción del proveedor con comunicación efectiva por parte del negocio. | **MEDIO** |
| | | Número de incidentes significativos por incumplimiento del proveedor en un periodo de tiempo. | **2** |
| *LOS INDICADORES CLAVE DE DESEMPEÑO DIRIGEN LAS METAS DE LOS PROCESOS* | | | |

| RESPECTO A LOS PROCESOS | | | |
|---|---|---|---|
| **METAS** | | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Establecer relaciones y responsabilidades bilaterales con proveedores calificados de servicios tercerizados.<br><br>2.- Monitorear la prestación del servicio y verificar el apego a los acuerdos.<br><br>3.- Asegurar que el proveedor cumple con los estándares internos y externos.<br><br>4.- Mantener el deseo del proveedor de continuar con la relación. | **SE MIDE CON** | Porcentaje de los principales proveedores que cumplen claramente los requerimientos definidos y los niveles de servicio. | **60%** |
| | | Número de controversias formales con el proveedor. | **1** |
| | | Porcentaje de facturas del proveedor en controversia. | **1%** |
| | | | |
| *LOS INDICADORES CLAVE DE PROCESOS DIRIGEN LAS METAS DE TI* | | | |

| RESPECTO A TI | | | |
|---|---|---|---|
| **METAS** | | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Asegurar una relación de mutua satisfacción con los terceros.<br><br>2.- Asegurar la satisfacción de los usuarios finales con las ofertas de servicio y los niveles de servicio.<br><br>3.- Asegurar transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI. | **SE MIDE CON** | Número de quejas de los usuarios debidas a los servicios contratados. | **5** |
| | | Porcentaje del gasto dedicado a aprovisionamiento competitivo. | **5%** |

### 3.1.4.5. NIVEL DE MADUREZ PROCESO DS2.




## NIVEL DE MADUREZ DETERMINADO

**DS2 Administrar los Servicios de Terceros: Básico** 2

### 3.1.4.6. RAZONES PARA DICHA EVALUACIÓN:

El proceso para supervisar a terceros proveedores de servicio, riesgos asociados y entrega de servicios es informal. Un contrato proforma firmado se usa con términos y condiciones estándar de ventas (por ej. la descripción de servicios que serán prestados). Los informes acerca de los servicios prestados están disponibles, pero los mismos no apoyan a los objetivos de negocio.

**Nivel Deseable.**

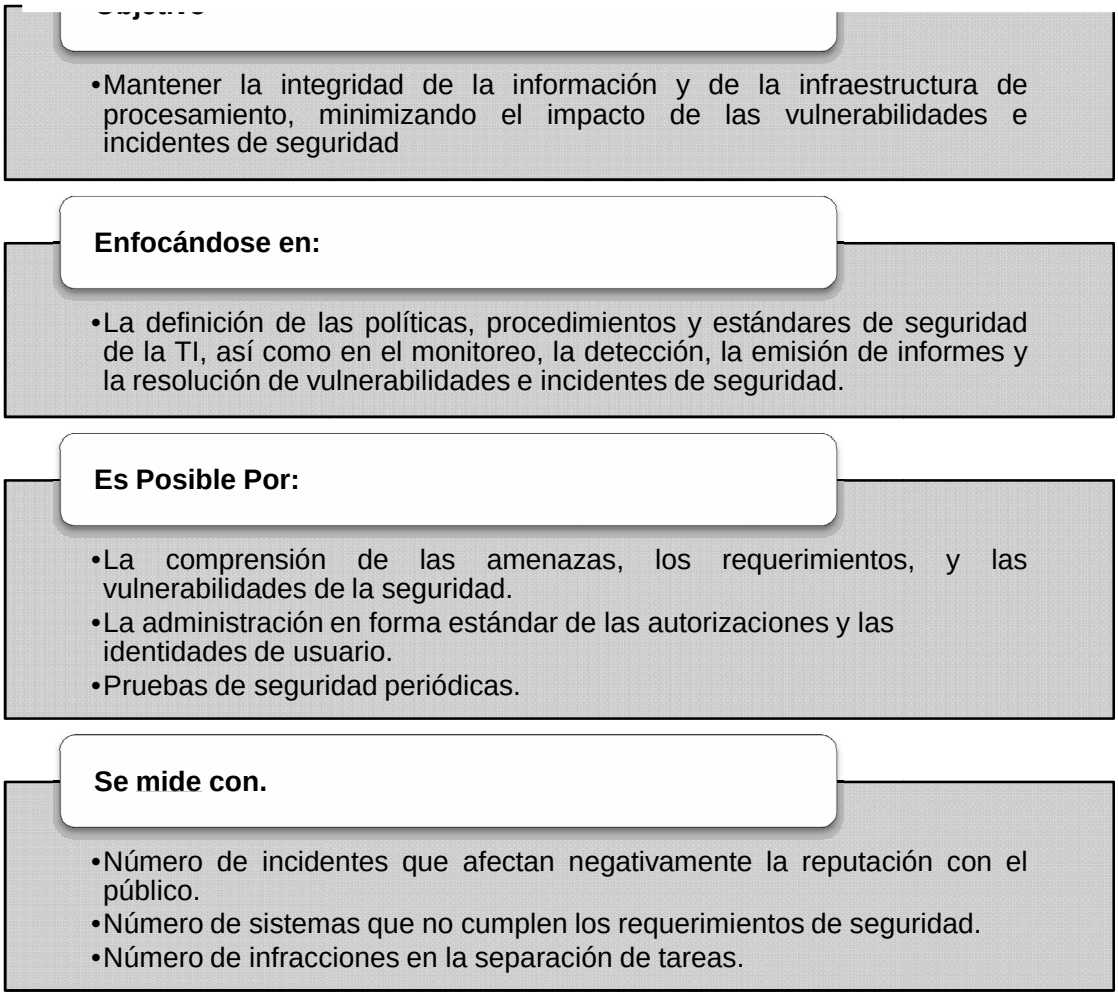

Salto Importante a la Formalidad : **Nivel Definido**

### 3.1.5. Auditoria Proceso DS5 - ASEGURAMIENTO DE LA SEGURIDAD DE LOS SISTEMAS

### Dominio : ENTREGA Y SOPORTE

### 3.1.5.1 INFORMACION

La necesidad de mantener la integridad de la información y de proteger los activos de TI exige un proceso de administración de la seguridad. Este proceso incluye establecer y mantener de roles y responsabilidades, políticas, estándares, y procedimientos de seguridad para la TI. La administración de la seguridad también incluye supervisiones de seguridad, pruebas periódicas y la implementación de acciones correctivas para atender las debilidades o los incidentes de seguridad identificados. Una administración eficaz de la seguridad protege a todos los activos de TI a fin de minimizar el impacto de negocio de las vulnerabilidades e incidentes de seguridad.



## PROCESO DS5 - ASEGURAMIENTO DE LA SEGURIDAD DE LOS SISTEMAS

### 3.1.5.2. OBTENCIÓN DEL ENTENDIMIENTO.

| | Descripción | Cumple | No Cumple |
|---|---|---|---|
| Entrevistas con: | Oficial de seguridad de mayor jerarquía de la organización | | X |
| | Administración de la seguridad en Ti y Gerencia de Sistemas | X | |
| | Administrador de la base de datos | X | |
| | Administrador de la seguridad en Ti | | X |
| | Administración del desarrollo de aplicaciones de Ti | | X |

| | | |
|---|---|---|
| Revisión de documentación de | Políticas y procedimientos para toda la organización referentes a la seguridad y el acceso de los sistemas de información. | NO |
| | Políticas y procedimientos de la Gerencia de Sistemas relacionadas con seguridad y acceso a los sistemas de información. | NO |

| | Descripción | Cumple | No Cumple |
|---|---|---|---|
| REVISAR : Políticas y procedimientos relevantes, así como requerimientos de seguridad de sistemas (normas legales y reglamentarias) incluyendo: | Procedimientos de administración de cuentas de usuario | SI | |
| | Política de seguridad del usuario o de protección de la información | SI | |
| | Estándares relacionados con el comercio electrónico | NO | |
| | Esquema de clasificación de datos | NO | |
| | Inventario de software de control de acceso | NO | |
| | Plano de los edificios/habitaciones que contienen recursos de sistemas de información | SI | |
| | Inventario o esquema de los puntos de acceso físico a los recursos de sistemas de información (por ejemplo, módems, líneas telefónicas y terminales remotas) | NO | |
| | Procedimientos de control de cambios del software de seguridad | NO | |
| | Procedimientos de seguimiento, solución y escalamiento de problemas | NO | |
| | Informes de violaciones a la seguridad y procedimientos de revisión gerencial. | NO | |
| | Inventario de dispositivos de cifrado de datos y de estándares de criptogrfía. | NO | |
| | Lista de los proveedores y clientes con acceso a los recursos del sistema. | NO | |
| | Lista de los proveedores de servicio utilizados en la transmisión de datos. | SI | |
| | Practicas de administración de redes relacionadas con pruebas de continuidad de la seguridad. | NO | |
| | Copias de los contratos con los proveedores del servicio de transmisión de datos. | NO | |
| | Copias de documentos firmados de seguridad y toma de conocimiento por los usuarios. | NO | |
| | Contenido del material de entrenamiento de seguridad para nuevos empleados | NO | |
| | Informes de auditoría de auditores externos, proveedores de servicios como terceras partes y dependencias gubernamentales relacionadas con la seguridad de los sistemas de la información | NO | |

### 3.1.5.3. EVALUACION OBJETIVOS DE CONTROL

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.1** Administración de la seguridad de TI | | | |
| **DESCRIPCION:** | | La seguridad de la TI debe gestionarse al nivel más alto de la organización apropiado, a fin de que la gestión de las acciones de seguridad estén en línea con los requerimientos de negocio | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿La seguridad de la TI se gestiona al nivel más alto de la organización apropiado, a fin de que la gestión de las acciones de seguridad esté en línea con los requerimientos de negocio? | La Gestión de Seguridad solo es conocida hasta el Nivel de la Gerencia de Sistemas, se evidenció que la Gerencia General No conoce del Tema de Seguridad de los sistemas | NO | | Pobre |
| 2 | ¿Los sistemas sensibles disponen de un entorno computacional aislado tal como el funcionamiento en una computadora dedicada, recursos compartidos solamente con los sistemas de confianza, etc.. | La empresa cuenta con un Centro de Procesamiento de Información con las debidas seguridad Físicas de Acceso | NO | | Satisfactorio |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.2** Plan de Seguridad de TI | | | |
| **DESCRIPCION:** | | Traducir en un plan global de seguridad de TI los requerimientos de información del negocio, la configuración de la TI, los planes de acción de riesgos de la información y la cultura de seguridad de la información. Implementar el plan global de seguridad de TI mediante políticas y procedimientos de seguridad así como con las inversiones adecuadas en servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a las partes interesadas y a los usuarios. | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se traducen en un plan global de seguridad de TI los requerimientos de información del negocio, la configuración de la TI, los planes de acción de riesgos de la información y la cultura de seguridad de la información? | La empresa no cuenta con un Plan de Seguridad de TI, solo cuentan con Procedimientos para tareas específicas | SI | | Pobre |
| 2 | ¿Se comunican las políticas y procedimientos de seguridad a las partes interesadas y a los usuarios? | Los Procedimientos Existentes son socializados a los empleados, pero solo para casos específicos | SI | | Satisfactorio |
| 3 | ¿Se implementa este plan mediante políticas y procedimientos de seguridad así como con las inversiones adecuadas en servicios, personal, software y hardware? | La empresa no cuenta con un Plan de Seguridad de TI, solo cuentan con Procedimientos para tareas específicas | NO | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.3** Administración de Identidad | | | |
| **DESCRIPCION:** | | Alinear los permisos de acceso de los usuarios a los sistemas y datos con las necesidades de negocio definidas y documentadas así como con los requerimientos de trabajo. Implementar y mantener vigentes medidas técnicas y de procedimiento costo-eficaces para establecer la identificación de los usuarios, implementar la autenticación y hacer valer los permisos de acceso. Mantener las identidades de usuario y los permisos de acceso en un repositorio central. Identificar unívocamente a todos los usuarios (internos, externos y temporales) y sus actividades en los sistemas de TI (aplicaciones de negocios, operación, desarrollo y mantenimiento del sistema). El propietario del sistema debe aprobar los permisos de acceso solicitados por la administración de usuarios y los mismos deben implementarse por la persona a cargo de la seguridad. | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se puede identificar unívocamente a todos los usuarios (internos, externos y temporales) y sus actividades en los sistemas de TI (aplicaciones de negocios, operación, desarrollo y mantenimiento del sistema)? | Existe un Inventario de los usuarios internos, y las Aplicaciones que utilizan. | SI | | Satisfactorio |
| 2 | ¿Los permisos de acceso de los usuarios a los sistemas y datos están en línea con las necesidades de negocio definidas y documentadas así como con los requerimientos de trabajo? | No Existe Documentación pero se evidenció que los permisos están asociados a las actividades que realiza cada usuario | NO | | Pobre |
| 3 | ¿El propietario del sistema aprueba los permisos de acceso solicitados por la administración de usuarios y los mismos son implementados por la persona a cargo de la seguridad? | Los Permisos son Administrados por los Propietarios del Sistema Jefe de Area, pero no es implementada por el Personal de Seguridad de IT. | NO | | Pobre |
| 4 | ¿Las identidades de usuario y los permisos de acceso se mantienen en un repositorio central? | Las Identidades de los Usuarios son Administrados por los Propietarios del Sistema, y se encuentran en cada Departamento | NO | | Pobre |
| 5 | ¿Se implementan y mantienen vigentes medidas técnicas y de procedimiento costo-eficaces para establecer la identificación de los usuarios, implementar la autenticación y hacer valer los permisos de acceso? | No Existe Procedimientos para la Identificación de usuarios | NO | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.3** Administración de Identidad | | | |
| 6 | ¿El acceso a sistemas de información es lograble solamente por medio de un proceso de logueo seguro? | Existe un Controlador de Dominio bajo Windows Server 2008, que realiza el Logueo seguro | NO | | Muy Bueno |
| 7 | ¿El método de la autenticación usado verifica la identidad del usuario demandada? Método comúnmente usado: contraseña que solamente el usuario sabe. | El Dominio de Windows, se encarga de solicitar a cada usuario modificar la Clave cada cierto período | NO | | Muy Bueno |
| 8 | ¿Existe un identificador único proporcionado a cada usuario ya sea operadores, administradores de sistema y el resto de personal incluyendo técnico? | Si Existe Identificador Único, pero no distingue el tipo de usuario | NO | | Pobre |
| 9 | ¿Existe un procedimiento para loguearse a un sistema de información? Éste debe reducir al mínimo la oportunidad del acceso desautorizado. | No Existe Documentación pero se evidenció que los permisos están asociados a las actividades que realiza cada usuario | SI | | Satisfactorio |
| 10 | ¿Existe un sistema de gestión de la contraseña que haga cumplir varios controles sobre la contraseña? Por ejemplo: la contraseña individual para responsabilidad, hace cumplir los cambios de la contraseña, las contraseñas en forma cifrada, no exhibir las contraseñas en la pantalla, etc.. | La Administración de Contraseñas realiza la Controladora de Dominio, Las Directivas son implementados por el Jefe de Sistemas de la Empresa | SI | | Satisfactorio |
| 11 | ¿La organización se asegura el obtener una clara descripción de las cualidades de seguridad de todos los servicios usados ya sean de redes públicas o privados? | No existe Información de las cualidades de seguridad de lo servicios usados | NO | | Pobre |
| 12 | ¿La política de control de accesos atiende a las reglas y los derechos para cada usuario o grupo de usuarios? | Las políticas de Control administra el controlador de Windows Server , pero para los usuarios en General. | SI | | Satisfactorio |
| 13 | ¿Los requisitos del negocio para con el control de accesos se han definido y documentado adecuadamente? | Los Controles de Acceso no están Definidos en función de los Requisitos del Negocio, es por medio de un procedimiento genérico | NO | | Pobre |
| 14 | ¿Los usuarios y proveedores de servicios recibieron una clara declaración de los requisitos del negocio a ser satisfecho por los controles de acceso? | Los Diferentes usuarios no recibieron la declaración de los Requisitos del Negocio | NO | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.4** Administración de Cuentas de Usuario | | | |
| **DESCRIPCION:** | | Efectuar periódicamente revisiones por parte de la Gerencia de todas las cuentas y los privilegios relacionados. Garantizar que la administración de las cuentas de usuarios maneja las cuentas que son solicitadas, establecidas, emitidas, suspendidas, modificadas y cerradas así como los privilegios de usuario relacionados. Incluir un procedimiento de aprobación que detalle quién es el propietario de los datos o del sistema que autoriza los privilegios de acceso. Asegurar que estos procedimientos se aplican a todos los usuarios, incluyendo los administradores (usuarios privilegiados) y a los usuarios internos y externos, aún en casos de emergencia. Disponer contractualmente los derechos y obligaciones relativos al acceso a la información y a los sistemas de la empresa. | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se garantiza que la administración de las cuentas de usuarios maneja las cuentas que son solicitadas, establecidas, emitidas, suspendidas, modificadas y cerradas así como los privilegios de usuario relacionados? | No Existe un Procedimiento de Administración de Cuentas de Usuario, Simplemente el Jefe Departamental Solicita Mediante Mail al Jefe de Sistemas la creación de una cuenta de Usuario determinada. | NO | | Pobre |
| 2 | ¿Se incluye un procedimiento de aprobación que detalla quién es el propietario de los datos o del sistema que autoriza los privilegios de acceso? | No Existe un Procedimiento de defina los propietarios de los Datos que autoricen los privilegios de Acceso | NO | | Pobre |
| 3 | ¿Estos procedimientos se aplican a todos los usuarios, incluyendo los administradores (usuarios privilegiados) y a los usuarios internos y externos, aún en casos de emergencia? | No Existe Procedimiento | NO | | Pobre |
| 4 | ¿Se disponen contractualmente los derechos y obligaciones relativos al acceso a la información y a los sistemas de la empresa? | Se Evidencia en el contrato del Trabajador un clausula de Confidencialidad de la información. | SI | | Satisfactorio |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.4** Administración de Cuentas de Usuario | | | |
| 5 | ¿Se efectúan periódicamente revisiones por parte de la Gerencia de todas las cuentas y los privilegios relacionados? | La Revisiones periódicas la realiza el Jefe de Sistemas, y solo comunica las novedades mas relevantes al Gerente de Sistemas | SI | | Muy Pobre |
| 6 | ¿Se ha renombrado la cuenta "Administrador" (Administrator)? | No se evidencia dicho Proceso | SI | | Satisfactorio |
| 7 | ¿La cuenta del usuario "root" está inhabilitada para que no se pueda hacer con ella un login directo sobre el sistema? | La cuenta root está habilitada pero solo es utilizada por el Administrador del Sistema | SI | | Satisfactorio |
| 8 | Las cuentas de usuarios que no están en uso, y particularmente las cuentas de "guest", "ftp", "mail", "bin" y "adm", ¿tienen todas ellas contraseña o están bloqueadas de modo que no sea posible loguearse al sistema a través de ninguna de ellas? | Todas la Cuentas tienes su respectiva Clave de Acceso y es Administrada por el Jefe de Sistemas | SI | | Satisfactorio |
| 9 | Aún en caso de estar trabajando con una facilidad de single sign-on, ¿se ha cambiado la contraseña que viene asignada por defecto para el usuario SYSTEM, que es MANAGER, por un valor no obvio, difícil de adivinar? | Todas las Cuentas han sido modificadas su contraseña no se evidencia que tengas claves por default | SI | | Satisfactorio |
| 10 | ¿Se exige un largo mínimo predeterminado para las contraseñas? | Las Políticas de Contraseñas las Administra el Controlador de Dominio de Windows Server | SI | | Satisfactorio |
| 12 | ¿Los administradores utilizan el "rconsole" solo en caso de que sea imprescindible? | No se evidencia dicho Proceso | NO | | Satisfactorio |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.4** Administración de Cuentas de Usuario | | | |
| 13 | ¿Existe algún procedimiento formal para el registro y eliminación de usuarios a los efectos de concederles el acceso a los servicios y sistemas de información multi-usuario? | No Existe Procedimiento para Registro y Eliminación de Usuarios | NO | | Satisfactorio |
| 14 | ¿Existe un proceso de autorización de la Gerencia para cada nuevo recurso de tratamiento de la información? Esto debe existir para todas las nuevas instalaciones tales como hardware y software. | No Existe Proceso documentado, pero todas las Instalaciones de Hardware y Software son autorizados por el Gerente de Sistemas | SI | | Pobre |
| 15 | ¿Existe un proceso para revisar los derechos de acceso de usuario en intervalos regulares de tiempo? Ejemplo: La revisión de privilegio especiales cada tres meses, privilegio normal cada seis meses. | Las Políticas de Acceso las Administra el Controlador de Dominio de Windows Server | SI | | Satisfactorio |
| 16 | ¿La asignación y la reasignación de contraseñas son controladas con un proceso de gestión formal? | No Existe Procedimiento de reasignación de Contraseñas. | NO | | Pobre |
| 17 | ¿La asignación y uso de cualquier privilegio en el ambiente de sistema multi-usuarios de información es restringido y controlado? | Se Evidencia el control de compartir la información a través del Proceso Compartir Recursos de Windows Server | SI | | Satisfactorio |
| 18 | ¿Se les solicita a los usuarios el firmar una declaración de confidencialidad de la contraseña? | No Solicitan al usuario firmar una Declaración de confidencialidad de contraseñas. | NO | | Pobre |

| | | | | |
|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.5** Pruebas, Vigilancia y Monitoreo de Seguridad | | |
| **DESCRIPCION:** | | Asegurar que el acceso a la información de registro esté en línea con los requerimientos de negocio en cuanto a los permisos de acceso y los requerimientos de vigencia. Debe existir una función de registro y monitoreo que permita detectar a tiempo actividades inusuales o anormales que puedan requerir atención. Asegurar que la implementación de la seguridad de TI se prueba y monitorea de forma pro-activa. Acreditar periódicamente la seguridad de la TI para garantizar que se mantiene el nivel de seguridad aprobado. | | |

| OC | METODOLOGIA | RESULTADO OBSERVADOS | EVIDENCIAS | | EVALUACION (Excelente , Muy Bueno, Satisfactorio, Pobre) |
|---|---|---|---|---|---|
| | | | DOCUMENTO | ANEXO | |
| 1 | ¿Se asegura que la implementación de la seguridad de TI se prueba y monitorea de forma pro-activa? | Existe un monitoreo al servidor Firewall, pero no con algún procedimiento o período establecido. | No | | Satisfactorio |
| 2 | ¿Se vuelve a acreditar periódicamente la seguridad de la TI para garantizar que se mantiene el nivel de seguridad aprobado? | No se cuenta con un Nivel de Seguridad Aprobado | No | | Pobre |
| 3 | ¿Existe una función de registro y monitoreo que permita detectar a tiempo actividades inusuales o anormales que puedan requerir atención? | A nivel de Firewall existe un análisis de los LOG, de accesos al servidor, pero no se establece el período en que realizan este proceso | No | | Satisfactorio |
| 4 | ¿El acceso a la información de registro está en línea con los requerimientos de negocio en cuanto a los permisos de acceso y los requerimientos de vigencia? | No Existe definido los permisos de acuerdo a los requerimientos del negocio. | No | | Pobre |
| 5 | ¿Existe un procedimiento de divulgación formal, para reportar incidentes en materia de seguridad a través de canales apropiados lo más rápidamente posible? | No Existe Procedimiento para informar los incidentes de seguridad que se puedan haber generado | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.5** Pruebas, Vigilancia y Monitoreo de Seguridad | | | |
| 6 | ¿Existe un procedimiento o una pauta formal para que los usuarios reporten debilidades en la seguridad, o amenazas, en los sistemas o servicios? | Formalmente no Existe un procedimiento para que los usuarios reporten anomalías de seguridad, pero si comunican fallos o anomalías detectadas mediante un correo | No | | Satisfactorio |
| 7 | ¿Existen los mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costos, de incidentes y malfuncionamientos? | No Existe Mecanismos que permitan cuantificar costos por incidentes y malfuncionamientos | No | | Pobre |
| 8 | ¿Existen los procedimientos para reportar cualquier malfuncionamiento del software? | No Existe Reporte formal, pero los usuarios reportan a TI el mal funcionamiento de algún tipo de Software | No | | Pobre |
| 9 | ¿Los expedientes importantes de la organización son protegidos contra la pérdida, destrucción y falsificación? | Los Expediente se encuentran en una caja de Seguridad | No | | Satisfactorio |
| 10 | ¿Los procedimientos están instalados para supervisar el uso de los sistemas de tratamiento de la información? | No Existe Procedimientos para supervisar el uso de Sistemas de Tratamiento de Información | No | | Pobre |
| 11 | ¿Los registros de auditoría que registran excepciones y otros acontecimientos relevantes a la seguridad son producidos y guardados por un período convenido para asistir, a futuro, a investigaciones y supervisión del control de acceso? | No se ha realizado Auditoria de Seguridad | No | | Pobre |
| 12 | ¿Los resultados de las actividades de supervisión son revisados regularmente? | Todas las actividades de supervisión son revisadas, pero no existe un período de tiempo definido | No | | Satisfactorio |

| | | |
|---|---|---|
| **DOMINIO:** | **DS** Entregar y Dar Soporte | |
| **PROCESO:** | **DS5** Garantizar la Seguridad en los Sistemas | |
| **OBJETIVO DE CONTROL:** | **DS.5.6** Definición de Incidente de Seguridad | |
| **DESCRIPCION:** | Asegurar que las características de los posibles incidentes de seguridad sean claramente definidas y comunicadas a fin de que los incidentes de seguridad puedan ser manejados por el proceso de gestión de incidentes y problemas. Asegurar que estas características incluyan una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Definir un número finito de niveles de impacto y para cada uno de ellos identificar las acciones específicas necesarias y las personas que deben ser notificadas. | |

| OC | METODOLOGIA | RESULTADO OBSERVADOS | EVIDENCIAS | | EVALUACION (Excelente , Muy Bueno, Satisfactorio, Pobre) |
|---|---|---|---|---|---|
| | | | DOCUMENTO | ANEXO | |
| 1 | ¿Se asegura que las características de los posibles incidentes de seguridad sean claramente definidas y comunicadas a fin de que los incidentes de seguridad puedan ser manejados por el proceso de gestión de incidentes y problemas? | No se han definido los incidentes de seguridad | No | | Pobre |
| 2 | ¿Estas características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto? | No se han definido los incidentes de seguridad | No | | Pobre |
| 3 | ¿Está definido un número finito de niveles de impacto y para cada uno de ellos están identificadas las acciones específicas necesarias y las personas que deben ser notificadas? | No se han definido los incidentes de seguridad | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.7** Protección de la Tecnología de la Seguridad | | | |
| **DESCRIPCION:** | | Asegurar que la tecnología importante relacionada con la seguridad es resistente a la manipulación y que la documentación de seguridad no se divulga innecesariamente, es decir, se mantiene un perfil bajo. Asegurar que la seguridad de los sistemas no dependan de que las especificaciones de seguridad sean secretas. | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se asegura que la tecnología importante relacionada con la seguridad es resistente a la manipulación y que la documentación de seguridad no se divulga innecesariamente, es decir, se mantiene un perfil bajo? | La Documentación de Seguridad que cuenta TI, tiene solo Accesos el Gerente de TI | No | | Satisfactorio |
| 2 | ¿La seguridad de los sistemas no depende de que las especificaciones de seguridad sean secretas? | La Seguridad de los Sistemas no depende de las especificaciones de seguridad. | No | | Satisfactorio |
| 3 | ¿La documentación de los sistemas es protegida contra accesos no autorizados? | Se evidencia que existe Documentación de fácil acceso a través de la Intranet | No | | Pobre |
| 4 | ¿La lista de acceso para la documentación de los sistemas es mantenida al mínimo y autorizada por el propietario de la aplicación? Ejemplo: la documentación del sistema debe ser mantenida en un disco compartido para propósitos específicos, el documento debe tener habilitadas listas de control de acceso (para ser accesible solamente por un número limitado de usuarios) | La Documentación se encuentra publicada en la Intranet y es de fácil acceso de los usuarios Internos | No | | Pobre |

| | | | | |
|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.8** Administración de Llaves Criptográficas | | |
| **DESCRIPCION:** | | Establecer políticas y procedimientos para organizar la generación, cambio, anulación, destrucción, distribución, certificación, almacenamiento, ingreso, uso y archivo de claves criptográficas a fin de garantizar la protección de las mismas respecto a su modificación o divulgación sin autorización. | | |

| OC | METODOLOGIA | RESULTADO OBSERVADOS | EVIDENCIAS | | EVALUACION (Excelente , Muy Bueno, Satisfactorio, Pobre) |
|---|---|---|---|---|---|
| | | | DOCUMENTO | ANEXO | |
| 1 | ¿Están establecidas políticas y procedimientos para organizar la generación, cambio, anulación, destrucción, distribución, certificación, almacenamiento, ingreso, uso y archivo de claves criptográficas a fin de garantizar la protección de las mismas respecto a su modificación o divulgación sin autorización? | No existe el sistema de Claves Criptográficas en los sistemas de la Empresa | No | | Pobre |
| 2 | ¿El sistema de gestión de llaves está basado en un conjunto de estándares, procedimientos y métodos acordados seguros? | No existe el sistema de Claves Criptográficas en los sistemas de la Empresa | No | | Pobre |
| 3 | ¿Existe un sistema de gestión para apoyar el uso en la organización de técnicas criptográficas, tales como técnica de llave secreta y llave pública? | No existe el sistema de Claves Criptográficas en los sistemas de la Empresa | No | | Pobre |
| 4 | ¿Son realizados relevamiento para analizar la sensibilidad de los datos y el nivel de protección necesaria? | No existe el sistema de Claves Criptográficas en los sistemas de la Empresa | No | | Pobre |
| 5 | ¿Son utilizadas firmas digitales para proteger la autenticidad e integridad de documentos electrónicos? | No existe el sistema de Claves Criptográficas en los sistemas de la Empresa | No | | Pobre |
| 6 | ¿Son utilizadas técnicas del cifrado para proteger los datos? | No existe el sistema de Claves Criptográficas en los sistemas de la Empresa | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.9** Prevención, Detección y Corrección de Software Malicioso | | | |
| **DESCRIPCION:** | | Garantizar la existencia en toda la empresa de medidas preventivas, de detección y corrección (particularmente las actualizaciones de seguridad y el control de virus) a fin de proteger los sistemas y la tecnología de la información del software malicioso (virus, gusanos, spyware, correo electrónico no solicitado, software fraudulento desarrollado internamente, etc.). | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se garantiza la existencia en toda la empresa de medidas preventivas, de detección y corrección (particularmente las actualizaciones de seguridad y el control de virus) a fin de proteger los sistemas y la tecnología de la información del software malicioso (virus, gusanos, spyware, correo electrónico no solicitado, software fraudulento desarrollado internamente, etc.)? | Existe un Sistema de Seguridad Apropiado, Firewall, Antivirus Administrado. | Si | | Muy Bueno |
| 2 | ¿Existe algún procedimiento para verificar que todos los boletines de alerta son exactos e informativos en lo que respecta al uso de software malicioso? | No Existe Procedimientos, pero si funciona un sistema de alertas al uso de software malicioso | Si | | Satisfactorio |
| 3 | ¿Existen controles contra el uso de software malicioso? | Existe Sistema Antivirus Centralizado, y Monitoreado | Si | | Muy Bueno |
| 4 | ¿Existen controles para asegurar que no son introducidos canales encubiertos y/o códigos Troyanos en sistemas nuevos o en sus actualizaciones? | No Existe Controles sobre los canales encubiertos | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.9** Prevención, Detección y Corrección de Software Malicioso | | | |
| 5 | ¿La política de seguridad trata asuntos de licenciamiento del software tales como prohibir el uso del software no autorizado? | Se Evidencia la prohibición del uso de Software no Autorizado | Si | | Muy Bueno |
| 6 | ¿Las actualizaciones de este software son obtenidas en forma regular para chequear los últimos virus? | Existe Sistema Antivirus Centralizado, y Monitoreado, y Actualizado | Si | | Muy Bueno |
| 7 | ¿Software antivirus está instalado en las computadoras para que cheque, aislé o remueva cualquier virus de la computadora o medios de almacenamiento? | Existe un Sistema de Antivirus, en cada computador, y administrados desde un Servidor de Seguridades | Si | | Muy Bueno |
| 8 | ¿Todo el tráfico originado por una red no-confiada es chequeado por virus dentro de la organización? Ejemplo: Comprobar si hay virus en el email, los archivos adjuntos del email y en la web, tráfico del FTP. | Existe un Sistema de Antivirus, en cada computador, y administrados desde un Servidor de Seguridades | Si | | Muy Bueno |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.10** Seguridad de la Red | | | |
| **DESCRIPCION:** | | Garantizar el empleo de técnicas de seguridad y procedimientos de gestión relacionados (por ej. firewalls, dispositivos de seguridad, segmentación de redes y detección de intrusión) a fin de autorizar el acceso y controlar el flujo de información desde y hacia las redes. | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se garantiza el empleo de técnicas de seguridad y procedimientos de gestión relacionados (por ej. firewalls, dispositivos de seguridad, segmentación de redes y detección de intrusión) a fin de autorizar el acceso y controlar el flujo de información desde y hacia las redes? | Existe Un Servidor Linux, con un Firewall implementado | Si | | Muy Bueno |
| 2 | ¿Existe algún control de la conexión a redes compartidas que se extienden más allá de los límites de organización? Ejemplo: correo electrónico, acceso a la web, transferencias de archivo, etc. , | El Control lo realiza el Firewall | No | | Satisfactorio |
| 3 | ¿Existe algún mecanismo de autentificación para las conexiones externas? Ejemplos: técnicas basadas en criptografía, dispositivos del hardware, software, protocolos de Challenge/Response, etc.. | No existe sistema de Autentificación, pero existe un Bloqueo de los Protocolos posibles de ataque | No | | Satisfactorio |
| 4 | ¿Existen controles especiales para salvaguardar la confidencialidad y la integridad del procesamiento de datos sobre las redes públicas y para proteger los sistemas conectados? Ejemplo: Redes privadas virtuales (VPN), otros mecanismos de cifrado y de hashing, etc. | Los Controles son realizados por el Firewall implementado bajo Linux | No | | Satisfactorio |
| 5 | ¿Fueron establecidas las responsabilidades y los procedimientos para la gestión del equipamiento remoto, incluyendo el equipamiento en áreas usuarias? | No Existe Procedimiento para Gestión de Equipamiento Remoto | No | | Pobre |
| 6 | ¿Fueron establecidos adecuados y eficaces controles operacionales como por ej. El separar la administración del sistema y de la red? | No existe este tipo de Controles Operacionales | No | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS5** Garantizar la Seguridad en los Sistemas | | | |
| **OBJETIVO DE CONTROL:** | | **DS.5.11** Intercambio de Datos Sensitivos | | | |
| **DESCRIPCION:** | | Garantizar que los datos de transacción sensibles se intercambian sólo a través de vías o medios confiables que cuentan con controles que proporcionan autenticidad de los contenidos, pruebas de envío, pruebas de recepción y reconocimiento de autoría. | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se garantiza que los datos de transacción sensibles se intercambian sólo a través de vías o medios confiables que cuentan con controles que proporcionan autenticidad de los contenidos, pruebas de envío, pruebas de recepción y reconocimiento de autoría? | El Sistema de Seguridad que cuenta la empresa no realiza control alguno de autenticidad de contenidos | No | | Pobre |
| 2 | ¿Es utilizado un mecanismo automático de identificación de terminales para autenticar conexiones? | No se evidencia mecanismo de Identificación de Terminales | No | | Pobre |
| 3 | ¿Existe algún control que restrinja la ruta entre el terminal del usuario y los servicios informáticos a los que el usuario está autorizado a tener acceso, Ejemplo: encaminamiento fijo para reducir el riesgo? | No existe Control de ruta entre terminales, Los usuarios están restringidos por Aplicación | No | | Pobre |
| 4 | ¿Existe alguna restricción en el tiempo de conexión para las aplicaciones de riesgo elevado? Este tipo de sistema se debe considerar para las aplicaciones sensibles para las cuales las terminales están instaladas en locaciones de riesgo elevado. | No Existe Clasificación de Aplicaciones por Tipo de Riesgo, por lo tanto no existe restricción de Tiempo de Conexión. | No | | Pobre |

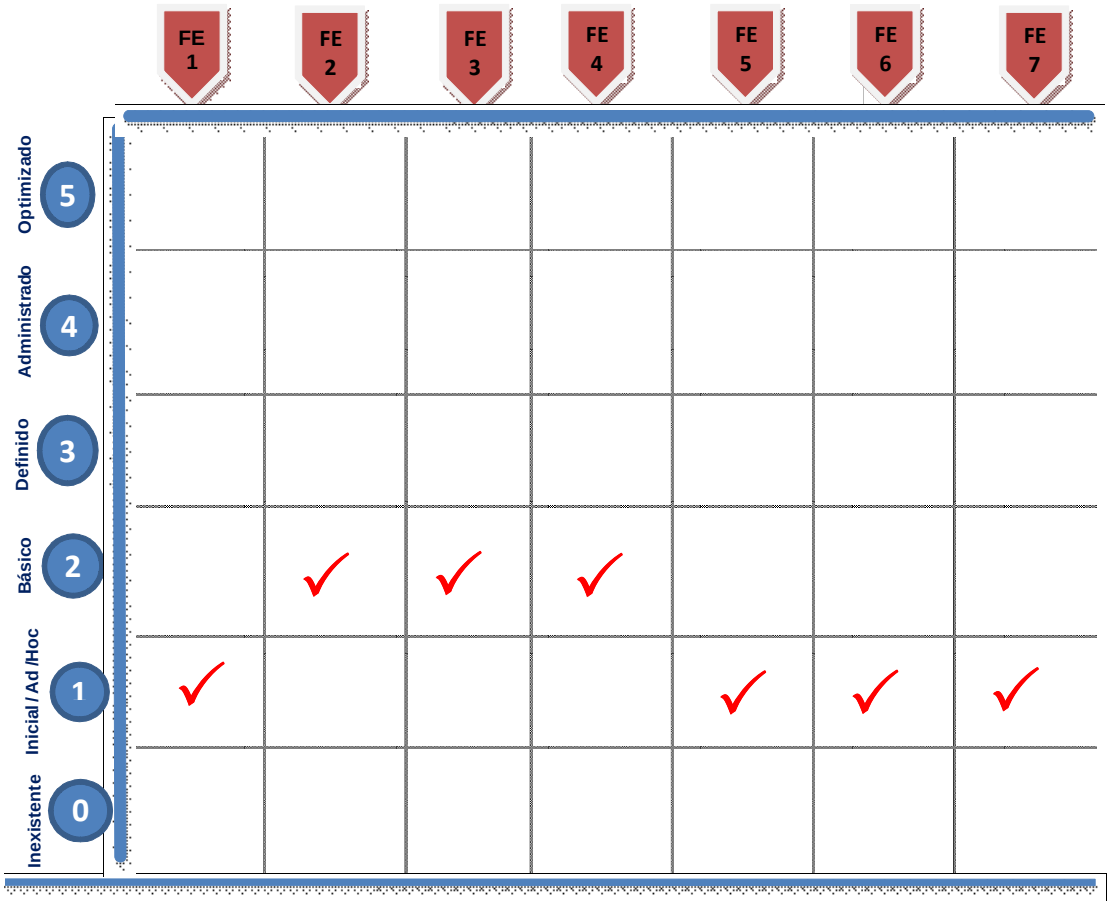
### 3.1.5.4. INDICADORES CLAVE DE DESEMPEÑO. KPI.

| RESPECTO A LAS ACTIVIDADES | | | |
|---|---|---|---|
| **METAS** | | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad. | **SE MIDE CON** | Frecuencia y revisión del tipo de eventos de seguridad a ser monitoreados. | **EVENTUAL** |
| 2.- Administración de las identidades y autorizaciones de los usuarios de manera estándar. | | Número y tipo de cuentas obsoletas. | **4** |
| 3.- Definición de incidentes de seguridad. | | Número de direcciones IP no autorizadas, puertos y tipos de tráfico denegados. | **10** |
| 4.- Pruebas de seguridad regulares. | | Porcentaje de llaves criptográficas comprometidas y revocadas. | **0** |
| | | Número de derechos de acceso autorizados, revocados, restaurados o cambiados. | **2** |
| *LOS INDICADORES CLAVE DE DESEMPEÑO DIRIGEN LAS METAS DE LOS PROCESOS* | | | |

| RESPECTO A LOS PROCESOS | | | |
|---|---|---|---|
| **METAS** | | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Permitir el acceso a información crítica y sensible solo a usuarios autorizados. | **SE MIDE CON** | Número y tipo de violaciones de acceso reales y sospechadas. | **15** |
| 2.- Identificar, monitorear y reportar vulnerabilidades e incidentes de seguridad. | | Número de violaciones en la segregación de funciones. | **0** |
| 3.- Detectar y resolver accesos no autorizados a la información, aplicaciones e infraestructura. | | Porcentaje de usuarios que no cumplen con los estándares de contraseñas. | **60%** |
| 4.- Minimizar el impacto de las vulnerabilidades y de los incidentes de seguridad. | | Número y tipo de código malicioso prevenido | **6** |
| | | | |
| *LOS INDICADORES CLAVE DE PROCESOS DIRIGEN LAS METAS DE TI* | | | |

| RESPECTO A TI | | | |
|---|---|---|---|
| **METAS** | | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Garantizar que la información crítica y confidencial esté prohibida a aquellos que no tienen acceso a ella. | **SE MIDE CON** | Número de incidentes con impacto al negocio. | **1** |
| 2.- Garantizar que las transacciones e intercambios de información automatizados del negocio sean confiables. | | Número de sistemas que no cumplen con los requerimientos de seguridad. | **2** |
| 3.- Mantener la integridad de la información y de la infraestructura de procesamiento. | | Tiempo para otorgar, cambiar o eliminar privilegios de acceso. | **180 m** |
| 4.- Proteger y mantener registro de todos los activos de TI. | | | |
| 5.- Garantizar que los servicios y la infraestructura de TI pueden resistir y recuperarse de fallas originadas por un error, ataque deliberado o desastre.. | | | |

### 3.4.5. NIVEL DE MADUREZ PROCESO DS5.




**NIVEL DE MADUREZ DETERMINADO**

**DS5 Garantizar la Seguridad en los Sistemas: Inicial** 1

### 3.4.6. RAZONES PARA DICHA EVALUACIÓN:

La organización reconoce la necesidad de la seguridad de TI. La conciencia de la seguridad depende de las personas. La seguridad de TI se atiende de forma reactiva. La seguridad de TI no se mide. Las violaciones de seguridad de TI detectadas provocan respuestas de asignación de culpas dado que las responsabilidades no están claras. Las respuestas a las violaciones de seguridad de TI son impredecibles.

Por ser una empresa pequeña, no existe un oficial de seguridades que desempeñe todas las funciones requeridas para garantizar la seguridad de los sistemas, sino que las mismas son realizadas por diferentes áreas, sin que se haya llegado a formalizar las responsabilidades para una ejecución efectiva, eficiente y documentada de actividades, y se asigne la rendición de cuentas de resultados y entregables.

**Recomendación:**

Formalizar en el manual de funciones las responsabilidades sobre la seguridad de TI, y establecer las políticas y procedimientos necesarios para administrarlas e implementarlas de forma clara, considerando la realización regular de un análisis de impacto y de riesgos de seguridad, y la ejecución de pruebas utilizando procesos estándares y formales que lleven a mejorar los niveles de seguridad. Para el efecto, se recomienda utilizar mejores prácticas internacionales que además promuevan la conciencia de la seguridad en toda la organización a través de programas de capacitación. Los reportes de

seguridad deben estar ligados con los objetivos del negocio y la capacitación sobre seguridad de TI debe ser planeada y administrada de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad.

**Nivel Deseable.**


Salto Importante a la Formalidad : **Nivel Definido**

### 3.1.6. Proceso: DS8 - GESTIÓN DE INCIDENTES Y DE LA MESA DE SOPORTE.

**Dominio : ENTREGA Y SOPORTE**

#### 3.1.6..1. INFORMACION

Es necesario un proceso de administración de la mesa de soporte e incidentes bien diseñado y ejecutado para poder proporcionar una respuesta oportuna y efectiva a las consultas y problemas de los usuarios de TI. Este proceso incluye la creación de una función de mesa de soporte con registros, un proceso de jerarquización de incidentes, análisis de tendencias y causas principales y resolución. Los beneficios de negocio incluyen un aumento en la productividad mediante la rápida solución a las consultas de los usuarios. Además, el negocio puede abordar las causas principales (como ser una capacitación deficiente de los usuarios) mediante una eficaz emisión de informes.

**Objetivo**

- Permitir el uso eficaz de los sistemas de TI al garantizar la resolución y el análisis de las consultas, preguntas e incidentes del usuario final.

**Enfocándose en:**

- Una función de mesa de soporte profesional con una rápida respuesta, claros procedimientos de escalamiento de incidentes y resolución y análisis de tendencias.

**Es Posible Por:**

- La instalación y operación de una mesa de soporte.
- El monitoreo y notificación de tendencias.
- La definición de Criterios y procedimientos claros para El escalamiento de incidentes.

**Se mide con.**

- Satisfacción del usuario con el soporte inicial.
- Porcentaje de incidentes resueltos dentro de un lapso de tiempo razonable o acordado.
- Índice de desistimiento de las llamadas.

### 3.1.6.2. OBTENCIÓN DEL ENTENDIMIENTO.

### PROCESO DS8 - GESTIÓN DE INCIDENTES Y DE LA MESA DE SOPORTE

| Categoría | Descripción | Cumple | No Cumple |
|---|---|---|---|
| Entrevistas con: | Administrador de la mesa de ayuda de TI | | X |
| | Usuarios seleccionados de los servicios de la información | X | X |
| | | Disponible | |
| Revisión de documentación de: | Políticas y procedimientos generales para la organización relacionados con el soporte a usuarios de la Gerencia de Sistemas | NO | |
| | Organigrama, misión, políticas y procedimientos de la Gerencia de Sistemas relacionados con las actividades de mesa de ayuda | SI | |
| | Informes relacionados con la consultas de los usuarios, su resolución y estadísticas de desempeño del mesa de ayuda | NO | |
| | Cualquier estándar de desempeño para las actividades del mesa de ayuda | NO | |
| | Acuerdos de nivel de servicios entre la Gerencia de Sistemas y usuarios diversos | NO | |
| | Archivos personales que muestren la formación y experiencia profesional del personal del mesa de ayuda | SI | |

### 3.1.6.3. EVALUACION OBJETIVOS DE CONTROL

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS8** Administrar la mesa de Servicio y los Incidentes | | | |
| **OBJETIVO DE CONTROL:** | | **DS.8.1** Mesa de soporte | | | |
| **DESCRIPCION:** | | Establecer una función de mesa de soporte, la cual funge como interfaz entre el usuario y la TI para registrar, comunicar, despachar y analizar todas las llamadas, los incidentes notificados, y las solicitudes de servicio y de información. Asegurar que existan procedimientos de monitoreo y escalamiento con base en los niveles de servicio acordados en relación al SLA adecuado que permitan la clasificación y priorización de cualquier asunto notificado, como ser un incidente o una solicitud de servicios o de información. Medir la satisfacción del usuario final con la calidad de la mesa de soporte y los servicios de TI. | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Está establecida una función de mesa de soporte, la cual funge como interfaz entre el usuario y la TI para registrar, comunicar, despachar y analizar todas las llamadas, los incidentes notificados, y las solicitudes de servicio y de información? | No se cuenta con un sistema Automatizado de Mesa de Soporte, esto se lo realiza de forma manual, en un registro diario de actividades realizadas y por realizar, mismas que se van cumpliendo en el transurso del día | NO | | Satisfactorio |
| 2 | ¿Existen procedimientos de monitoreo y escalamiento con base en los niveles de servicio acordados en relación al SLA adecuado que permiten la clasificación y priorización de cualquier asunto notificado, como ser un incidente o una solicitud de servicios o de información? | No existe acuerdos SLA, la clasificación y priorización de asuntos o actividades lo hace el técnico de soporte de acuerdo a su criterio basandose de acuerdo al funcionamiento de la empresa para el correcto desempeño de la misma. | NO | | Satisfactorio |
| 3 | ¿Se mide la satisfacción del usuario final con la calidad de la mesa de soporte y los servicios de TI? | Se lo realiza parcialmente haciendo un seguimiento mediante llamadas o visita personal al puesto de trabajo, en el cual se verifica que el soporte o solucion brindado ha sido lo correcto. | NO | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS8** Administrar la mesa de Servicio y los Incidentes | | | |
| **OBJETIVO DE CONTROL:** | | **DS.8.2** Registro de consultas de clientes | | | |
| **DESCRIPCION:** | | Asegurar que esta función trabaje en estrecha relación con los procesos como ser la gestión de incidentes, problemas, cambios, capacidad y disponibilidad. Clasificar los incidentes de acuerdo a la prioridad de negocio y de servicios, transfiriéndolos al equipo de gestión de problemas adecuado y manteniendo a los clientes informados acerca del estado de sus consultas. Establecer una función y un sistema para permitir el registro y seguimiento de las llamadas, incidentes, solicitudes de servicio y de información. | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Están establecidos una función y un sistema para permitir el registro y seguimiento de las llamadas, incidentes, solicitudes de servicio y de información? | No existe función ni sistema, tampoco se lo hace de ninguna forma | NO | | Pobre |
| 2 | ¿Esta función trabaja en estrecha relación con los procesos como ser la gestión de incidentes, problemas, cambios, capacidad y disponibilidad? | No existe la función, por lo tanto no es posible responder | NO | | Pobre |
| 3 | ¿Los incidentes se clasifican de acuerdo a la prioridad de negocio y de servicios, siendo transferidos al equipo de gestión de problemas adecuado y manteniendo a los clientes informados acerca del estado de sus consultas? | Si se realiza la clasificación de acuerdo a la prioridad del negocio, y son transferidos al personal competente. | NO | | Satisfactorio |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS8** Administrar la mesa de Servicio y los Incidentes | | | |
| **OBJETIVO DE CONTROL:** | | **DS.8.3** Escalamiento de incidentes | | | |
| **DESCRIPCION:** | | Garantizar que la titularidad y el monitoreo del ciclo de vida de los incidentes permanece en la mesa de soporte para los incidentes ocasionados por los usuarios sin importar qué grupo de TI esta trabajando para resolver los mismos. Establecer los procedimientos de la mesa de soporte de forma que los incidentes que no puedan ser resueltos de inmediato sean escalados adecuadamente de acuerdo a los límites definidos en el SLA y, si correspondiese, se proporcionen soluciones alternativas o temporales. | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Se establecen los procedimientos de la mesa de soporte de forma que los incidentes que no puedan ser resueltos de inmediato sean escalados adecuadamente de acuerdo a los límites definidos en el SLA y, si correspondiese, se proporcionan soluciones alternativas o temporales? | No existe un procedimiento definido actualmente, en tales casos si se brinda solución a los incidentes siempre dando una solucion temporal o alternativas que ayuden a los usuarios | NO | | Satisfactorio |
| 2 | ¿Se garantiza que la titularidad y el monitoreo del ciclo de vida de los incidentes permanece en la mesa de soporte para los incidentes ocasionados por los usuarios sin importar qué grupo de TI esta trabajando para resolver los mismos? | Si todo permanece en la mesa de trabajo hasta que se llegue a dar una solución definitiva al incidente, sin importar el personal de IT que trabaje en ello | NO | | Satisfactorio |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS8** Administrar la mesa de Servicio y los Incidentes | | | |
| **OBJETIVO DE CONTROL:** | | **DS.8.4** Cierre de incidentes | | | |
| **DESCRIPCION:** | | Deben existir procedimientos establecidos para el monitoreo oportuno de la resolución de las consultas de los usuarios. Una vez resuelto el incidente, la mesa de soporte debe registrar la causa principal, si se conoce la misma, y confirma que la acción tomada fue acordada con el cliente. | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Existen procedimientos establecidos para el monitoreo oportuno de la resolución de las consultas de los usuarios? | No se cuenta con procedimientos para realizar este monitoreo, los usuarios son quienes al brindarle una solución dejan de informar sobre el incidente y por tanto se toma como concluido. | NO | | Satisfactorio |
| 2 | Una vez resuelto el incidente, ¿la mesa de soporte registra la causa principal, si se conoce la misma, y confirma que la acción tomada fue acordada con el cliente? | No se realiza ningun registro acerca de la resolución del incidente | NO | | Pobre |

| | | | | | |
|---|---|---|---|---|---|
| **DOMINIO:** | | **DS** Entregar y Dar Soporte | | | |
| **PROCESO:** | | **DS8** Administrar la mesa de Servicio y los Incidentes | | | |
| **OBJETIVO DE CONTROL:** | | **DS.8.5** Análisis de tendencias | | | |
| **DESCRIPCION:** | | Generar informes acerca de la actividad de la mesa de soporte para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta del mismo así como para identificar tendencias o problemas recurrentes, de forma de poder mejorar continuamente el servicio. | | | |
| **OC** | **METODOLOGIA** | **RESULTADO OBSERVADOS** | **EVIDENCIAS** | | **EVALUACION** (Excelente , Muy Bueno, Satisfactorio, Pobre) |
| | | | **DOCUMENTO** | **ANEXO** | |
| 1 | ¿Existen procedimientos establecidos para el monitoreo oportuno de la resolución de las consultas de los usuarios? | No existe un monitoreo para monitorear las consultas de los usuarios | NO | | Pobre |
| 2 | Una vez resuelto el incidente, ¿la mesa de soporte registra la causa principal, si se conoce la misma, y confirma que la acción tomada fue acordada con el cliente? | No Existe Sistema de Registro de Incidentes, peor aun el registros del seguimiento | NO | | Pobre |

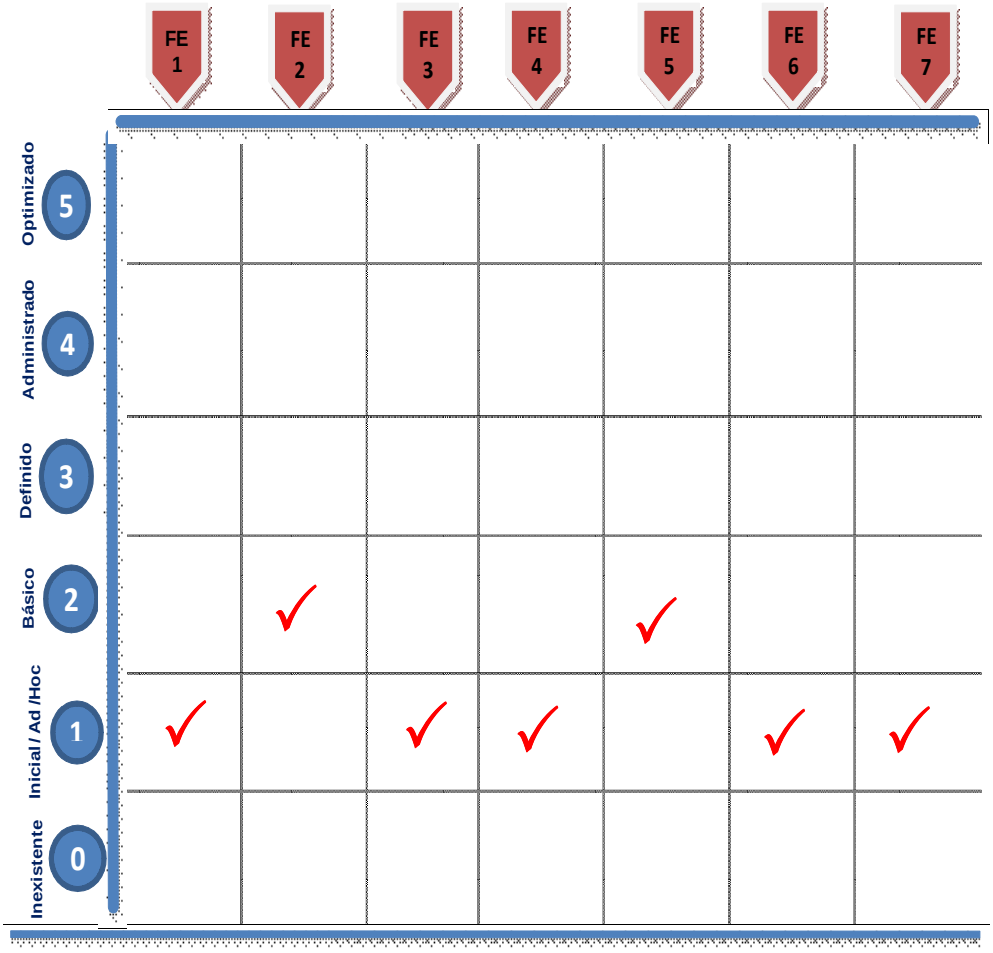
### 3.1.6.4. INDICADORES CLAVE DE DESEMPEÑO. KPI.

| RESPECTO A LOS PROCESOS | | | |
|---|---|---|---|
| **METAS** | | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Analizar, documentar y escalar incidentes de manera oportuna. | **SE MIDE CON** | Porcentaje de resoluciones en la primera línea de atención con base en el total de peticiones. | **60%** |
| 2.- Responder a las consultas de forma precisa y oportuna. | | Porcentaje de incidentes reabiertos. | **10%** |
| 3.- Llevar a cabo de manera regular análisis de tendencias de incidentes y consultas. | | Índice de abandono de llamadas. | **5%** |
| | | Duración promedio de los incidentes por severidad. | **8d** |
| | | Velocidad promedio para responder a peticiones vía teléfono y vía web o e-mail. | **6h** |
| | | | |
| *LOS INDICADORES CLAVE DE PROCESOS DIRIGEN LAS METAS DE TI* | | | |

| RESPECTO A LAS ACTIVIDADES | | | |
|---|---|---|---|
| **METAS** | | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Instalación y operación de una mesa de servicios. | **SE MIDE CON** | Porcentaje de incidentes y de solicitudes de servicio reportadas y registradas usando herramientas automatizadas. | **10%** |
| 2.- Monitoreo y reporte de tendencias. | | Número de días de entrenamiento del personal de la mesa de servicios por año. | **15** |
| 3.- Alineación de las prioridades de resolución con las prioridades del negocio. | | Número de llamadas atendidas por el personal de la mesa de servicios por hora. | **5** |
| 4.- Definición de procedimientos y criterios de escalamiento claros. | | Porcentaje de incidentes que requieren soporte local (en campo, visita personal). | **60%** |
| | | Acumulación de consultas sin resolver. | **3** |
| *LOS INDICADORES CLAVE DE DESEMPEÑO DIRIGEN LAS METAS DE LOS PROCESOS* | | | |

| RESPECTO A TI | | | |
|---|---|---|---|
| **METAS** | | **INDICADOR CLAVE DE DESEMPEÑO** | **VALOR** |
| 1.- Garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio.<br><br>2.- Garantizar el uso y desempeño apropiados de las aplicaciones y soluciones tecnológicas.<br><br>3.- Garantizar que los servicios de TI estén disponibles cuando se requieran. | **SE MIDE CON** | Satisfacción del usuario con el soporte de primera línea (mesa de servicios o base de conocimientos). | **Satisfactorio** |
| | | Porcentaje de incidentes resueltos dentro de un período de tiempo aceptable/ acordado. | **50%** |
| | | | |

### 3.1.6.5. NIVEL DE MADUREZ PROCESO DS8.



### 3.1.6.5 NIVEL DE MADUREZ DETERMINADO

**DS8 Administrar la mesa de Servicio y los Incidentes**: **Inicial** 


### 3.1.6.6. RAZONES PARA DICHA EVALUACIÓN:

La gerencia reconoce que se necesita un proceso asistido por herramientas y personal para responder a las consultas de los usuarios y para administrar la resolución de problemas. No hay sin embargo un proceso estandarizado y solo se proporciona soporte reactivo. La gerencia no monitorea las consultas de los usuarios, los problemas o las tendencias. No hay un proceso de jerarquización para garantizar que los problemas sean resueltos.

**Nivel Deseable.**


Salto Importante a la Formalidad : **Nivel Definido**

## 3.2. RESULTADOS AUDITORIA

### 3.2.1 DEFINICIÓN DE NIVELES DE MADUREZ E IMPACTO EN EL NEGOCIO

| *Dominios y Procesos de Tecnología de Cobit 4.1* | | | Nivel Actual | Causa | Nivel Objetivo | Causa | Brecha | Impacto | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | A | M | B |
| PLANEAR Y ORGANIZAR | **PO9** | *Evaluar y administrar los riesgos de TI* | **0** | No Existe una metodología formal para la identificación de riesgos tecnológicos por lo que su administración se realiza de manera intuitiva | **2** | Definir una Metodología Formal para Administrar el Riesgo y al menos aplicar a los proyectos importantes . Los procesos de mitigación de riesgos deben ser implementados donde se identifiquen los riesgos. | **2** | | **X** | |
| | **PO10** | *Administrar proyectos* | **1** | Los roles y responsabilidades de la administración de proyectos no están definidos. Los proyectos, cronogramas e hitos de los mismos están pobremente definidos. El tiempo y los gastos del personal del proyecto no son seguidos y comparados con los presupuestos. | **2** | Recursos Limitados para poder conformar el área de Proyectos, directamente lo realiza el Gerente de Sistemas. La empresa debe iniciar con el proceso de desarrollar y utilizar ciertas técnicas y métodos de un proyecto a otro. Los proyectos de TI deben definirce de manera formal objetivos de negocio y técnicos. | **1** | | | **X** |

| Dominios y Procesos de Tecnología de Cobit 4.1 | | | Nivel Actual | Causa | Nivel Objetivo | Causa | Brecha | Impacto | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | A | M | B |
| ENTREGARY DARSOPORTE | **DS2** | *Administrar los servicios de terceros* | **2** | El proceso para Administración de proveedores de servicio,es informal. El contrato firmado se usa con términos y condiciones estándar de ventas . Los informes acerca de los servicios prestados están disponibles, pero los mismos no apoyan a los objetivos de negocio. | **3** | Se debe Establecer procedimientos bien documentados para administrar los servicios prestados por terceros, con procesos claros para la autorización y negociación con los proveedores. La naturaleza de los servicios a ser prestados deben ser detallados en el contrato e incluir requerimientos operativos, legales y de control. Los términos contractuales se deben basar en plantillas estandarizadas. | **1** | | | **X** |
| | **DS5** | *Garantizar la seguridad de los sistemas* | **1** | La empresa reconoce la necesidad de la seguridad de TI. La seguridad de TI se atiende de forma reactiva. La seguridad de TI no se mide. Las violaciones de seguridad de TI detectadas provocan respuestas de asignación de culpas dado que las responsabilidades no están claras. | **3** | Concientizar a gerencia. Definir la política de seguridad de TI, Establecer procedimientos de seguridad de TI alineados con la política de seguridad. Establecer responsabilidades de seguridad de TI. Definir un plan de seguridad de TI de acuerdo al análisis del riesgo. Establecer pruebas de seguridad ad hoc. Definir plan de capacitación en seguridad. | **2** | **X** | | |
| | **DS8** | *Administrar la mesa de servicio y los incidentes* | **1** | No existe personal y herramientas automatizadas para responder a las consultas de los usuarios y para administrar la resolución de problemas. El proceso no está estandarizado y solo se proporciona soporte reactivo. No existe seguimiento a las consultas y problemas de los usuarios. No hay un proceso de jerarquización para garantizar que los problemas sean resueltos. | **3** | Implementación de una mesa de soporte y de un proceso de administración de incidentes. Los procedimientos deben ser estandarizados y documentados. Desarrollar una Base de datos con una lista de preguntas frecuentes (FAQs) y de directrices de usuario. Realizar Seguimiento a Las consultas y los incidentes. Los usuarios deben recibir instrucciones claras respecto a dónde y cómo informar acerca de los problemas e incidentes. | **2** | **X** | | |

### 3.2.2 HALLAZGOS RELEVANTES

A continuación se detalla el análisis efectuado a cada uno de los procesos de tecnología de información cuya situación es relevante para la institución.

Las observaciones se encuentran agrupadas por el nivel de riesgo alcanzado por los procesos, y las recomendaciones han sido efectuadas considerando el nivel de madurez objetivo definido por la institución, y los aspectos que permitirían mitigar los riesgos tecnológicos a los que se encuentran expuestos actualmente cada uno de los procesos de tecnología de información, en base a las mejores prácticas sugeridas por Cobit 4.1.

#### 3.2.2.1 Procesos con Impacto alto.

No existe procesos con Riesgo Alto

#### 3.2.2.2 Procesos con Impacto Medio para la Empresa.

**• PO9 Evaluar y administrar los riesgos de TI**

La debilidad en la evaluación y administración de los riesgos de TI se encuentra en la falta de definición formal de los roles y responsabilidades sobre el mismo, pues actualmente una parte lo ejecuta el Jefe de Sistemas , pero dichas funciones no han sido formalizadas en el manual orgánico funcional, lo que dificulta el análisis y comunicación de riesgos tecnológicos y

su impacto potencial en las metas y procesos de negocio, e impide realizar un seguimiento de su ejecución y que ésta sea efectiva, eficiente y documentada para la rendición de cuentas de resultados y entregables . Además, no existe una metodología formal para la identificación de riesgos tecnológicos por lo que su administración se realiza de manera intuitiva y se podría dar una evaluación incompleta de los mismos.

***Recomendación:***

Establecer las políticas de administración de riesgos la definición de cuándo y cómo realizar las evaluaciones de riesgos, en base algún Estándar Internacional para la administración de riesgos con el objetivo de garantizar que todos los riesgos claves sean identificados; documentar el proceso de administración de riesgos y hacerlo disponible para todo el personal involucrado.

Elaborar las descripciones de puestos para las responsabilidades de administración de riesgos, incluyendo la rendición de cuentas y los entregables.

**Plan de acción:**

La Gerencia de Sistemas deberá presentar una propuesta para dar cumplimiento a la recomendación efectuada hasta diciembre del 2012, para

someterlo a revisión y aprobación del Comité de Operaciones hasta enero del 2013. Coordinar con el Jefe de Seguridad y Salud del Trabajo quien ya tienen elaborado las descripciones de puestos para definir las responsabilidades de la administración de riesgos, hasta enero del 2013.

**• DS5 Garantizar la seguridad de los sistemas**

Por cuanto el Departamento de Tecnología y Sistemas es pequeño, no existe un oficial de seguridades que desempeñe todas las funciones requeridas para garantizar la seguridad de los sistemas, sino que las mismas son realizadas por el Gerente de Sistemas, sin que se haya llegado a formalizar las responsabilidades para una ejecución efectiva, eficiente y documentada de actividades, y se asigne la rendición de cuentas de resultados y entregables.

**Recomendación:**

Elaborar el manual de funciones las responsabilidades sobre la seguridad de TI, y establecer las políticas y procedimientos necesarios para administrarlas e implementarlas de forma clara, considerando la realización regular de un análisis de impacto y de riesgos de seguridad, y la ejecución de pruebas utilizando procesos estándares y formales que lleven a mejorar los niveles de seguridad. Para el efecto, se recomienda utilizar mejores prácticas

internacionales que además promuevan la conciencia de la seguridad en toda la organización a través de programas de capacitación.

**Plan de acción:**

Elaborar un cronograma para la ejecución de todas las actividades recomendadas a partir de Enero del 2013 y hasta el primer semestre.

**• DS8 Administrar la mesa de servicio y los incidentes.**

El Departamento de TI no tiene personal asignado específicamente para este proceso y además no existe herramientas automatizadas para responder a las consultas de los usuarios y para administrar la resolución de problemas. El proceso no está estandarizado y solo se proporciona soporte reactivo. No existe seguimiento a las consultas y problemas de los usuarios. No hay un proceso de jerarquización para garantizar que los problemas sean resueltos.

**Recomendación:**

Desarrollar un esquema de Mesa de Ayuda para la empresa, con base en las mejores prácticas de ITIL, proveerá a la institución de procesos y procedimientos basados en las mejores prácticas mundiales de este tipo de servicios, orientándolos a optimizar el servicio de soporte a usuarios y mejorar la satisfacción del mismo.

Desarrollar una Propuesta para la Implementación de la Mesa de Ayuda basada en el Marco ITIL y aplicada a la Infraestructura de la empresa

**Plan de acción:**

Elaborar un cronograma para la ejecución de todas las actividades recomendadas a partir de Junio del 2012 y hasta el primer semestre.

# CAPITULO 4

## *4. PROYECTOS DE INVERSION*

### *4.1 INTRODUCCION*

En la actualidad toda organización exitosa se ha concientizado de la importancia del manejo de las tecnologías de información (TI), especialmente en la implementación de nuevos proyectos tecnológicos que incluye costos y beneficios, pero que mejora la producción y competitividad.

La empresa CAVES SA EMA, fué objeto de una Auditoria de riesgos informáticos utilizando Cobit como marco de Referencia, en donde se obtuvieron los resultados que permitieron identificar el Nivel de Madurez que se encuentra los diferentes procesos COBIT seleccionados, adicionalmente se emitieron recomendaciones para la implementación de diversos proyectos tecnológicos y de gestión se pretenden disminuir la brecha existente entre el Nivel de madurez actual y el propuesto a alcanzar.

El presente trabajo tiene por objeto presentar Proyectos de Inversión de Tecnología para los procesos Auditados con mayor impacto en la empresas para que mediante su la implementación disminuya la brecha de Nivel de Madurez identificada .

A continuación se detalla los Proyectos a presentar.

**Tabla 4.1: Proyectos de Inversión para Procesos Auditados**

| PROCESO | | Nivel Actual | Nivel Objetivo | Se Requiere | Secuencia Proyecto a Ejecutar | PROYECTO PROPUESTO |
|---|---|---|---|---|---|---|
| PO9 | *Evaluar y administrar los riesgos de TI* | 0 | 2 | Definir una Metodología Formal para Administrar el Riesgo . Los procesos de mitigación de riesgos deben ser implementados donde se identifiquen los riesgos. | 1 | IMPLEMENTACION DE MAGERIT COMO UNA SOLUCION PARA EL ANALISIS Y GESTION DE RIESGOS. |
| DS5 | *Garantizar la seguridad de los sistemas* | 1 | 3 | Definir la política de seguridad de TI, Establecer procedimientos de seguridad de TI alineados con la política de seguridad. Establecer responsabilidades de seguridad de TI. Definir un plan de seguridad de TI de acuerdo al análisis del riesgo. Definir plan de capacitación en seguridad. | 2 | ELABORACIÓN DE UN PLAN DE GESTION DE SEGURIDAD BASADO EN LA NORMA ISO/IEC 17799:2005 |
| DS8 | *Administrar la mesa de servicio y los incidentes* | 1 | 3 | Implementación de una mesa de soporte y de un proceso de administración de incidentes. Los procedimientos deben ser estandarizados y documentados. Desarrollar una Base de datos con una lista de preguntas frecuentes (FAQs) y de directrices de usuario. Realizar Seguimiento a Las consultas y los incidentes. | 3 | IMPLEMENTACION DE SYSID COMO UNA SOLUCION DE MESA DE AYUDA BASADO EN LAS MEJORES PRÁCTICAS DE ITIL. |

La Tabla representa los Procesos Cobit de Mayor impacto a la empresa Auditada, con los niveles de madurez Actual como el Objetivo a alcanzar, mediante la implementación del proyecto propuesto, adicionalmente se detalla la secuencia en que se debería ejecutar los Proyectos.

### *4.2 METAS DEL PROYECTO*

Presentar tres Proyectos de Inversión tecnológica, anteriormente enumerados, en donde se define los Objetivos, metodología a utilizar, se detalla los Recursos Humanos, Materiales, Actividades a ejecutarse, y la Gestión Económica del proyecto.

## 4.3 PROYECTO 1: IMPLEMENTACION DE MAGERIT COMO UNA SOLUCION PARA EL ANALISIS Y GESTION DE RIESGOS.

### 4.3.1 DELIMITACION

**CAMPO** **:** Proyecto De Inversión
**AREA** **:** Plan de Negocios. Tecnología
**UBICACION** **:** Departamento de Tecnología y Sistemas de la Empresa CAVES SA EMA, PLANTA CENTRAL - Tumbaco
**FECHA** **:** 2012/Julio

### 4.3.2 JUSTIFICACION

De acuerdo a los resultados de la Auditoría realizada al Departamento de Sistemas utilizando COBIT como marco de Referencia , se evidenció que Departamento de TI no cuenta con una metodología formal para la identificación de riesgos tecnológicos por lo que su administración se realiza de manera intuitiva.

Aceptando la recomendación emitida en la Auditoría realizada se plantea un Proyecto para definir una Metodología Formal de Administración de Riesgos y al menos aplicar a los proyectos importantes . Los procesos de mitigación de riesgos deben ser implementados donde se identifiquen los riesgos.

### 4.3.3 OBJETIVO GENERAL.

Implementar Magerit como una Metodología para el Análisis y Gestión de Riesgos aplicada a la infraestructura de la empresa CAVES que permita disminuir la Brecha del Nivel de Madurez actual en relación con el Nivel Objetivo, definido en los resultados de la Auditoría Realizada.

### 4.3.4 JUSTIFICACION METODOLOGICA

#### 4.3.4 .1 Evaluación y Análisis de Riesgos

Análisis de riesgos - Es una consideración sistemática:

- Se estima el impacto potencial de una falla de seguridad en los negocios y sus posibles consecuencias de pérdida de la confidencialidad, integridad o disponibilidad
- Se evalúa la probabilidad de ocurrencia de dicha falla tomando en cuenta las amenazas, vulnerabilidades y controles implementados.
- Establecimiento de PRIORIDADES y ACCIONES

Para la realización de un AGR existen varias guías informales, aproximaciones metódicas, estándares y herramientas de soporte que buscan gestionar y mitigar los riegos. Las principales metodologías de análisis y gestión de riesgos de uso habitual en el mercado de la seguridad de la información son: MAGERIT, OCTAVE, CRAMM, IRAM, para determinar cuál es la metodología que genere confianza en la mitigación de riesgos se ha realizado la siguiente tabla comparativa.

| | | MAGERIT | OCTAVE | CRAMM | IRAM |
|---|---|---|---|---|---|
| **ALCANCE CONSIDERADO** | Análisis de Riesgos | ● | ● | ● | ● |
| | Gestión de Riesgos | ● | ● | ● | ● |
| **TIPO DE ANALISIS** | Cuantitativo | ● | ⊙ | ● | ● |
| | Cualitativo | ● | ⊙ | ● | ● |
| | Mixto | ● | ⊙ | ○ | ○ |
| **TIPO DE RIESGOS** | Intrínseco | ● | ○ | ● | ● |
| | Efectivo | ● | ● | ● | ● |
| | Residual | ● | ⊙ | ○ | ⊙ |

**Figura 4.1: Gráfico Comparación Metodologías para AGR**

| | | | | | |
|---|---|---|---|---|---|
| **ELEMENTOS DEL MODELO** | Procesos | ● | ● | ○ | ○ |
| | Activos | ● | ● | ● | ● |
| | Recursos | ● | ● | ○ | ○ |
| | Dependencias | ● | ● | ● | ● |
| | Vulnerabilidades | ● | ● | ● | ● |
| | Amenazas | ● | ● | ● | ● |
| | Salvaguardas | ● | ● | ● | ● |
| **OBJETIVOS DE SEGURIDAD** | Confidencialidad | ● | ● | ● | ● |
| | Integridad | ● | ● | ● | ● |
| | Disponibilidad | ● | ● | ● | ● |
| | Autenticidad | ● | ● | ● | ● |
| | Trazabilidad | ● | ○ | ○ | ○ |
| **INVENTARIOS** | Tipos de Recursos | ● | ● | ● | ○ |
| | Vulnerabilidades | ● | ● | ● | ● |
| | Amenazas | ● | ● | ● | ● |
| | Salvaguardas | ◉ | ● | ○ | ● |
| **AYUDAS A LA IMPLANTACION** | Herramienta | ● | ● | ● | ● |
| | Plan de Proyecto | ● | ● | ⊙ | ○ |
| | Técnicas | ● | ● | ○ | ○ |
| | Roles | ● | ● | ● | ○ |
| | Comparativas | ● | ○ | ● | ○ |
| | Otros | ○ | Cuestionarios | Cuestionarios | Soporte del ISF |

Del análisis comparativo realizado, se concluye que MAGERIT versión 2, es una metodología confiable, completa con una herramienta propia, que no da lugar a la improvisación, ni dependa de la arbitrariedad del analista.
Es completa por que tiene procesos, actividades, tareas y una herramienta propia desarrollado bajo su metodología.

#### 4.3.4.2 Descripción de la Metodología Magerit

La metodología MAGERIT versión 2, se ha estructurado en tres libros:

1. Método.
2. Catálogo de Elementos.
3. Guía de Técnicas.

Estos permiten desarrollar un análisis y gestión de riesgos de una manera técnica, con el objetivo de guiar en el trascurso del proyecto, a continuación se realiza un breve resumen de los libros en mención.

**LIBRO UNO: MÉTODO.**

El libro Uno conocido como **Método**, se estructura desde tres perspectivas:

1. “Describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación. Es una presentación netamente conceptual.

2. Describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, normalizar actividades, hitos y documentación para que la realización del proyecto esté bajo control en todo momento.

3. Aplica la metodología al caso del desarrollo de sistemas de información, en el que los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el inicio, tanto los riesgos a que están expuestos, como los riesgos que las propias aplicaciones introducen en el sistema” .

**LIBRO DOS: CATÁLOGO DE ELEMENTOS.**

El libro Dos conocido como Catálogos de Elementos, se estructura desde dos perspectivas:

1. “Facilitar la labor de las personas que desarrollan el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.

2. Homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos” .

**LIBRO TRES: GUÍA DE TÉCNICAS**

La Guía de Técnicas, sugiere que se aplique técnicas específicas y generales, para la elaboración de proyectos de análisis y gestión de riesgos. Además es una guía de consulta en las diferentes tareas que contiene dicho proyecto.

Del análisis comparativo realizado, se concluye que MAGERIT versión 2, es una metodología confiable, completa con una herramienta propia, que no da lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Es completa por que tiene procesos, actividades, tareas y una herramienta propia desarrollado bajo su metodología.

### 4.3.4.3. Justificación Herramienta Software

En la selección de la herramienta para el AGR, para el presente proyecto, se elabora un análisis comparativo de las herramientas disponibles en el mercado, como se observa a continuación en la tabla.

**Tabla 4.2: Comparación Herramientas Software para AGR**

| *HERRAMIENTA* | *INSTITUCION O EMPRESA* | *METODOLOGIA* | *LICENCIA PRIVADA* | *IDIOMAS* | *ESTANDARES* | *MODELO DE MADUREZ* |
|---|---|---|---|---|---|---|
| **CRAMM EXPERT** | Siemens Enterprise Communications | Evaluación de Riesgo de CRAMM | SI | Ingles Holandés Checo | ISO 27001 | No |
| **TOOLKIT SRM** | Security Risk Management | - | SI | Inglés Portugués | ISO 27000 | No |
| **RISICARE** | CLUSIF | MEHARI | SI | Francés Inglés | ISO/IEC 17799 ISO/IEC 27001 | No |
| **RMStudio** | STIKI | - | SI | Inglés | ISO 27000 | No |
| **ORICO** | SOMAP.ORG | OGRCM3 | Open Source | Español Inglés | - | No |
| **PILAR** | GOBIERNO ESPAÑOL | MAGERIT | SI | Español Inglés | ISO/IEC 27001/2005 ISO/IEC 15408/2005 ISO/IEC 17799/2005 ISO/IEC 13335/2005 | CMMI |

Del análisis comparativo, se selecciona la herramienta PILAR, por las siguientes razones:

1. Contiene los modelos de madurez de la CMMI.

2. Se basa en una metodología aceptada en la Unión Europea.

3. Se basa en normas, estándares, código de buenas prácticas de la gestión de la seguridad de la información, como la ISO 17799:2005, Código de buenas prácticas para la Gestión de la Seguridad de la información

Para la utilización de la herramienta PILAR, es necesario disponer de una licencia de uso, COMERCIAL

**BENEFICIOS**

PILAR reducida a la mínima expresión para realizar análisis de riesgos muy rápidos. El resultado del análisis puede cargarse en PILAR para un estudio más detallado.

µPILAR se distribuye con perfiles específicos. Sólo se pueden analizar los perfiles de la distribución.

Se analizan los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (accountability).

Para tratar el riesgo se proponen salvaguardas (o contra medidas), analizándose el riesgo residual.

**PROVEEDORES**

Empresa: EAR / PILAR Tipo de Proveedor: Fabricante Consultor tecnológico

Dirección: Juan Esplandiú, 12 Localidad: 28007 Madrid Provincia: Madrid

url: **www.ar-tools.com**

e-mail: info@ar-tools.com Tfno/Fax: 607733894 /

### 4.3.5 APLICACION METODOLOGICA

Para la realización del proyecto de AGR, se debe implementar 3 procesos, con sus actividades y tareas respectivas.

**PROCESO P1. PLANIFICACION:**

Se describirá la situación actual del Departamento de tecnología y Sistemas, su infraestructura, activos recurso, etc.

**PROCESO P2. ANALISIS DE RIESGOS.**

Este proceso , tiene como objetivo identificar y valorar los activos y amenazas que tiene la empresa, como también estimar el impacto y el riesgo de la materialización de las amenazas sobre los activos,

Para la elaboración de las tareas del proceso dos “Análisis de riesgos”, se debe trabajar en conjunto e integradamente con los dos libros restantes de la metodología MAGERIT; “Catálogo de elementos” y la “Guías de Técnicas”, los que contienen los diferentes catálogos y técnicas para poder realizar el AGR del presente proyecto.

La metodología MAGERIT, recomienda realizar cinco pasos, en el análisis de riesgos, como se observa en la figura 4.2, que manifiesta que se debe tratar primero los pasos 1, 2, 4 y 5, obviando el paso 3, de forma que las valoraciones del impacto y/o riesgos son realizadas sin salvaguardadas desplegadas, con el objetivo de obtener estimaciones realistas del impacto y/o riesgo potencial.

Una vez obtenido este escenario, se incorporan las salvaguardas del paso 3 de forma que las valoraciones del impacto y/o riesgos son realizadas sin salvaguardadas desplegadas, con el objetivo de obtener estimaciones realistas del impacto y/o riesgo potencial.

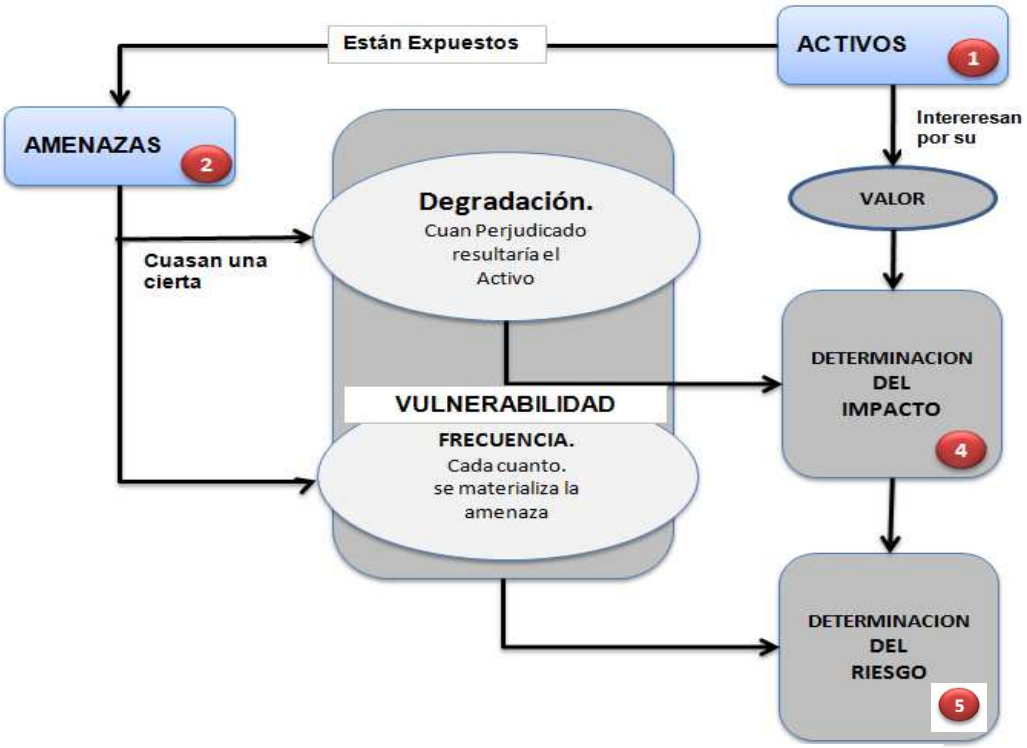



**Figura 4.2: MAGERIT – Proceso Análisis de Riesgos**

Para poder alcanzar dichos objetivos se deben implementar las siguientes actividades y tareas como se describen a continuación:

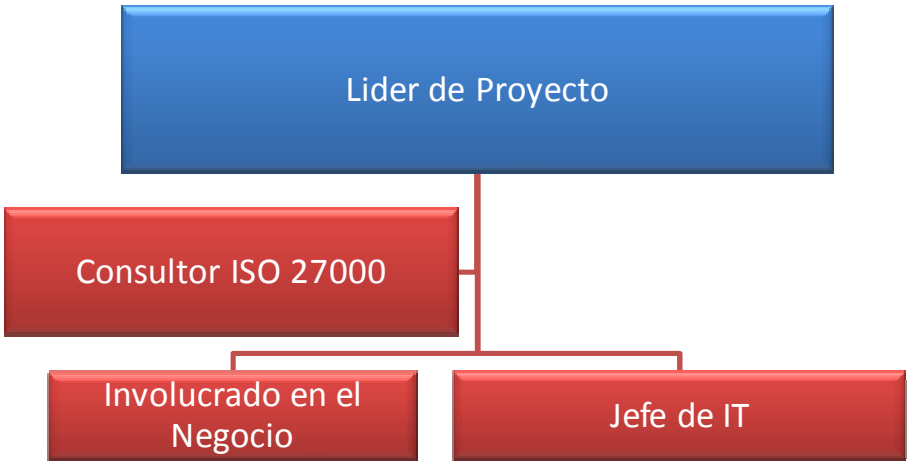
| **PROCESO:** | **P2** ANALISIS DE RIESGOS | | | |
|---|---|---|---|---|
| **ACTIVIDAD:** | **A2.1**: Caracterización de los activos. | | | |
| **DESCRIPCION:** | Se identifica los activos relevantes de la institución para su análisis por el tipo de activos, identificando las relaciones entre los diferentes activos, determinando en que dimensiones de seguridad son importantes y valorarlos, para la realización de está actividad se realiza las siguientes tareas | | | |
| **TAREA** | | **RESULTADOS A OBTENER** | **HERRAMIENTA** | **OBSERVACION** |
| A.2.1.1 | Identificación de los activos. | Relación y Caracterización de los Activos | PILAR | Al activo se le relaciona con la clase de activo a la que pertenece dentro de su respectiva capa |
| A.2.1.2 | Dependencias entre activos | Diagrama de Dependencia entre activos | PILAR | |
| A.2.1.3 | Valoración de los Activos | Informe del Modelo de Valor | PILAR | Utilizar los criterios de valoración |

| **PROCESO:** | **P2** ANALISIS DE RIESGOS | | | |
|---|---|---|---|---|
| **ACTIVIDAD:** | **A2.2**: Caracterización de las amenazas. | | | |
| **DESCRIPCION:** | Identifica las posibles amenazas que se pueden materializar sobre los activos anteriormente identificados, considerando la degradación y la frecuencia de dichos activos | | | |
| **TAREA** | | **RESULTADOS A OBTENER** | **HERRAMIENTA** | **OBSERVACION** |
| A.2.2.1 | Identificación de las amenazas. | Identificación de Amenazas, relevantes sobre cada activo | PILAR | Utilizar Catálogo de amenazas del libro dos; Catálogo de Elementos y las técnicas árboles de ataques y valoración Delphi del libro tres Guías Técnicas |
| A.2.2.2 | Valoración de las amenazas | Catálogo de valoración de las amenazas | PILAR | |

| | | | | |
|---|---|---|---|---|
| **PROCESO:** | **P2** ANALISIS DE RIESGOS | | | |
| **ACTIVIDAD:** | **A2.4**: Estimación del estado de riesgo | | | |
| **DESCRIPCION:** | Procesar todos los datos recopilados en las actividades anteriores. Con la finalidad de obtener el informe del estado de riesgo | | | |
| **TAREA** | | **RESULTADOS A OBTENER** | **HERRAMIENTA** | **OBSERVACION** |
| A.2.4.1 | Estimación del impacto | Informe de Impacto acumulado y residual por activo | PILAR | El informe completo del impacto acumulado y residual se encuentra en el informe "Análisis del Impacto". |
| A.2.4.3 | Interpretación de los resultados | Informe priorizado de activos con respecto al mayor impacto y/o riesgo | PILAR | |
| A.2.4.2 | Estimación del riesgo. | Informe de riesgo potencial y residual por activo. | PILAR | |

| | | | | |
|---|---|---|---|---|
| **PROCESO:** | **P2** ANALISIS DE RIESGOS | | | |
| **ACTIVIDAD:** | **A2.3**: Caracterización de las salvaguardas | | | |
| **DESCRIPCION:** | Identifica las salvaguardas a desplegar en la empresa y su eficacia en la mitigación del riesgo ocasionado por la materialización de las amenazas sobre los activos de la empresa. | | | |
| **TAREA** | | **RESULTADOS A OBTENER** | **HERRAMIENTA** | **OBSERVACION** |
| A.2.3.1 | Identificación de las salvaguardas existentes | Catálogo de las salvaguardas | PILAR | Se implementa la técnica del árbol de ataques del libro tres Guías Técnicas |
| A.2.3.2 | Valoración de las salvaguardas existentes. | Catálogo de las salvaguardas | PILAR | |

### 4.3.6 ORGANIGRAMA DEL PROYECTO.




| CARGO | PERFIL | FUNCIONES |
|---|---|---|
| **Lider Proyecto** | Ing Sistemas con experiencia en proyectos medianos y manejo de personal | Administrar el Proyecto |
| **Consultor ISO 27000** | Consultor con Amplios Conocimientos en la Norma ISO 27000 | Dar soporte en el area |
| **Involucrado en el Negocio** | Persona con amplios conocimientos en todos los procesos del Negocio | Proporciona información acerca del nivel de riesgo que se considera aceptable. Proporciona información de históricos que sirvan de ayuda para la identificación de los riesgos del proyecto. |
| **Jefe de IT** | Ingeniero en Sistemas con conocimientos en Seguridad de la Información | Desarrolla y mantiene el plan de gestión de riesgos. Durante el proyecto debe llevar a cabo la monitorización y control de los riesgos de los que es responsable, mandar las actualizaciones de su registro al jefe de proyecto y de escalar situaciones excepcionales al jefe de proyecto |

### 4.3.7 BIENES A ADQUIRIR PARA EL PROYECTO

## Organización de Recursos

| BIENES A ADQUIRIR PARA EL PROYECTO | |
|---|---|
| **SOFTWARE** | |
| **DESCRIPCION** | **COSTO TOTAL** |
| **Licencia Comercial EAR / PILAR** | |
| Análisis de riesgos cualitativo<br>Análisis de riesgos cuantitativo<br>Análisis de impacto y continuidad de operaciones<br>1 perfil de evaluación | 1.842,00 |
| Soporte base de datos (SQL) | 614,10 |
| | |
| **SUBTOTAL:** | **2.456,10** |
| **TOTAL DE BIENES A ADQUIRIR:** | **2.456,10** |

## 4.3.8 ORGANIZACIÓN DE LOS RECURSOS.

| RECURSOS HUMANOS PROPIOS QUE INTERVENDRAN EN EL PROYECTO | | | | | |
|---|---|---|---|---|---|
| **NOMBRE Y APELLIDO** | **PROFESION U OFICIO** | **FUNCION EN EL PROYECTO** | **SUELDO MENSUAL** | **NUMERO DE MESES** | **COSTO TOTAL** |
| | Ing. Sistemas | Lider de proyecto | 1.800,00 | 4 | 0,00 |
| | Ing. Sistemas | Ingeniero en Sistemas | 1.200,00 | 2 | 0,00 |
| | | Involucrado en el Negocio | 1.200,00 | 4 | 0,00 |
| | | | | **SUBTOTAL:** | **0,00** |

| CONSULTORIA Y SERVICIOS TECNOLOGICOS A CONTRATAR | | | |
|---|---|---|---|
| **DESCRIPCION** | **COSTO MENSUAL** | **NUMERO DE MESES** | **COSTO TOTAL** |
| Consultor Experto ISO 27000 | 2.000,00 | 2 | 4.000,00 |
| Capacitación en ISO 27000 Personal IT | 1.200,00 | 1 | 1.200,00 |
| | | | |

| **TOTAL DE CONSULTORIA Y SERVICIOS TECNOLOGICOS A CONTRATAR:** | **5.200,00** |
|---|---|

| MATERIALES E INSUMOS | | | | |
|---|---|---|---|---|
| DETALLE | UNIDAD DE MEDIDA | CANTIDAD | COSTO UNITARIO | COSTO TOTAL |
| Papel | Resma | 5,00 | 8,00 | 40,00 |
| Toner | Cartucho | 1,00 | 90,00 | 90,00 |
| Pizarra | Unidades | 1,00 | 60,00 | 60,00 |
| Marcadores Tiza liquida | Marcador | 5,00 | 1,50 | 7,50 |
| Scanner | Unidad | 1,00 | 200,00 | 200,00 |
| Esferos | Unidad | 10,00 | 0,50 | 5,00 |
| | | | | 0,00 |
| | | | | 0,00 |
| **TOTAL DE MATERIALES E INSUMOS:** | | | | **402,50** |

| RESUMEN CONSOLIDADO | | |
|---|---|---|
| DESCRIPCIONES | RESUMEN DE CUADROS | RESUMEN DE COSTOS |
| BIENES | 2.456,10 | 2.456,10 |
| RECURSOS HUMANOS | 0,00 | 0,00 |
| CONSULTORIAS Y SERVICIOS | 5.200,00 | 5.200,00 |
| MATERIALES E INSUMOS | 402,50 | 402,50 |
| TOTALES | 8.058,60 | 8.058,60 |

| Duración del proyecto | 4 | meses |
|---|---|---|

| COSTO TOTAL | Mes 1 al 4 | | | | | | |
|---|---|---|---|---|---|---|---|
| DESCRIPCION | 1 | 2 | 3 | 4 | | | TOTAL |
| BIENES DE CAPITAL | 614,03 | 614,03 | 614,03 | 614,03 | | | 2.456,10 |
| RECURSOS HUMANOS | 0,00 | 0,00 | 0,00 | 0,00 | | | 0,00 |
| CONSULTORIAS Y SERVICIOS | 3.200,00 | 2.000,00 | | | | | 5.200,00 |
| MATERIALES E INSUMOS | 100,63 | 100,63 | 100,63 | 100,63 | | | 402,50 |
| TOTALES | 3.914,65 | 2.714,65 | 714,65 | 714,65 | | | 8.058,60 |

## 4.3.9 PLANIFICACION TEMPORAL

| DESCRIPCION DE LAS ETAPAS | |
|---|---|
| CODIGO ETAPA | DESCRIPCION |
| A | PROCESO P1: PLANIFICACIÓN |
| B | PROCESO P2: ANÁLISIS DE RIESGOS |
| C | PROCESO P3: GESTION DE RIESGOS |
| D | CIERRE DEL PROYECTO |

**DESCRIPCION DE LAS ACTIVIDADES DENTRO DE LA ETAPA**

| | | | MES 1 | | | | MES 2 | | | | MES 3 | | | | MES 4 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CODIGO ETAPA | CODIGO ACTIVIDAD | DESCRIPCION | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 |
| A | 1 | Actividad A1.1: Estudio de oportunidad | | | | | | | | | | | | | | | | |
| A | 2 | Actividad A1.2: Determinación del alcance del proyecto | | | | | | | | | | | | | | | | |
| A | 3 | Actividad A1.3: Planificación del proyecto | | | | | | | | | | | | | | | | |
| A | 4 | Actividad A1.4: Lanzamiento del proyecto | | | | | | | | | | | | | | | | |
| B | 1 | Actividad A2.1: Caracterización de los activos: | | | | | | | | | | | | | | | | |
| B | 2 | Actividad A2.2: Caracterización de las amenazas. | | | | | | | | | | | | | | | | |
| B | 3 | Actividad A2.4: Estimación del estado de riesgo. | | | | | | | | | | | | | | | | |
| B | 4 | Actividad A2.3: Caracterización de las salvaguardas. | | | | | | | | | | | | | | | | |
| C | 1 | ACTIVIDAD A3.1: Toma de decisiones. | | | | | | | | | | | | | | | | |
| C | 2 | ACTIVIDAD A3.2: Elaboración Plan de Mitigación | | | | | | | | | | | | | | | | |
| D | 1 | Reporte Cierre y entrega de Documentación | | | | | | | | | | | | | | | | |
| D | 2 | Cierre formal del proyecto (carta de finiquito) | | | | | | | | | | | | | | | | |

## 4.4 PROYECTO 2: ELABORACION DE UN PLAN DE GESTION DE SEGURIDAD BASADO EN LA NORMA ISO/IEC 17799-2005

### 4.4.1 DELIMITACION

**CAMPO :** Proyecto De Inversión
**AREA :** Plan de Negocios. Tecnología
**UBICACION :** Departamento de Tecnología y Sistemas.
CAVES SA EMA, PLANTA CENTRAL
Tumbaco - Quito - Ecuador

### 4.4.2 JUSTIFICACION

Actualmente, el departamento de TI de la Empresa Caves sa ema. no cuenta con un marco de referencia para delinear un Sistema de Gestión de Seguridad que se ajuste a las actividades de la empresa.

De acuerdo a las recomendaciones realizadas en la Auditoría realizada al Departamento de Sistemas utilizando COBIT como marco de Referencia , se menciona definir la política de seguridad de TI, Establecer procedimientos de seguridad de TI alineados con la política de seguridad. Establecer responsabilidades de seguridad de TI. Definir un plan de seguridad de TI de acuerdo al análisis del riesgo.

Para el efecto, se recomienda utilizar la Norma ISO/IEC 17799 que promueven la conciencia de la seguridad en toda la organización a través de programas de capacitación.

Dicho Plan permitirá asegurar la protección de la información e incrementar la confianza de todas las personas vinculadas a la empresa.

### 4.4.3 OBJETIVO GENERAL.

Formular una propuesta de Plan de Gestión de Seguridad de la Información basada en TIC's para la Empresa CAVES SA EMA, utilizando el estándar ISO/IEC 27001:2005, que permita disminuir la Brecha del Nivel de Madurez actual en relación con el Nivel Objetivo

### 4.4.4 MARCO TEORICO

#### 4.4.4.1 Conceptos Básicos.

**La Información:** "La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada." ISO/IEC 17799

**Vulnerabilidad:** Una debilidad (o agujero) en la seguridad de la organización

- Puntos y control de acceso (lógicos y físicos)
- Falta de Mantenimiento
- Personal sin conocimiento
- Desactualización de los sistemas críticos

*Una vulnerabilidad, por sí misma, no produce daños. Es un condicionante para que una amenaza afecte un activo.*

**Amenaza :** Declaración intencionada de hacer un daño (Virus, acceso no autorizado, robo). Las amenazas se pueden materializar y transformarse en agresiones.

**Riesgo:** Potencial explotación de una vulnerabilidad de un activo de información por una amenaza.

**Ataque:** Acción intencional e injustificada (desde el punto de vista del atacado). Intento por romper la seguridad de un sistema o de un componente del sistema.

**LA SEGURIDAD**

- Es difícil de medir, la mayor parte del tiempo oímos de ella cuando solo cuando falla
- La medición de los resultados es clave para justificar la inversión ante la alta gerencia
- La Seguridad es una sensación y una realidad. Sentirse seguro no es realmente estar protegido.
- El concepto de seguridad es altamente subjetivo, por tanto cada uno determina su nivel de riesgo y lo que está dispuesto a dar por las medidas que tome.
- No hay un nivel correcto de seguridad, existe un juicio personal sobre el nivel de riesgo aceptable y lo que constituye una amenaza.

## SEGURIDAD DE LA INFORMACIÓN.

El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

## CONCEPTO:

La seguridad de la información se define como la preservación de:

- Confidencialidad. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
- Integridad. Garantía de la exactitud y totalidad de la información y de los métodos de procesamiento.
- Disponibilidad. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y a los recursos relacionados.

## OBJETIVOS:

- Asegurar la continuidad de la empresa.
- Mantener la competitividad, la rentabilidad, los recursos generales, el cumplimiento de las leyes y la imagen comercial.
- Minimizar el riesgo.
- Maximizar las oportunidades del negocio.

### 4.4.5 JUSTIFICACIÓN METODOLÓGICA

#### 4.4.5.1 Norma ISO 17799

ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

Existen multitud de estándares aplicables a diferentes niveles pero ISO 17799 como estándar internacional, es el más extendido y aceptado.

**Objetivo de la norma ISO 17799**

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones de confianza entre las empresas.

#### 4.4.5.2 Sistema de Gestión de la Seguridad de la Información (SGSI)

- La norma ISO 17799 recoge la relación de controles a aplicar (o al menos, a evaluar) para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI)
- Conjunto completo de controles que conforman las buenas prácticas de seguridad de la información.
    - Redactada de forma flexible e independiente de cualquier solución de seguridad concreta.
    - Proporciona buenas prácticas neutrales con respecto a tecnologías o fabricantes específicos.

#### 4.4.5.3 Estructura Norma ISO 17799:2005

La norma ISO 17799:2005 establece once dominios de control que cubren por completo la Gestión de la Seguridad de la Información:

1. **Política de seguridad:** Dirigir y dar soporte a la Gestión de la seguridad de la información -directrices y recomendaciones-
2. **Aspectos organizativos de la seguridad:** Gestión dentro de la Organización (recursos, activos, tercerización, etc.)
3. **Clasificación y control de activos**: Inventario y nivel de protección de los activos.
4. **Seguridad ligada al personal:** Reducir riesgos de errores humanos, robos, fraudes o mal uso de los recursos.
5. **Seguridad física y del entorno:** Evitar accesos no autorizados, violación, daños o perturbaciones a las instalaciones y a los datos
6. **Gestión de comunicaciones y operaciones**: Asegurar la operación correcta y segura de los recursos de tratamiento de información.
7. **Control de accesos:** Evitar accesos no autorizados a los sistemas de información (de usuarios, computadores, redes, etc).
8. **Desarrollo y mantenimiento de sistemas:** Asegurar que la seguridad está incorporada dentro de los sistemas de información. Evitar pérdidas, modificaciones, mal uso.
9. **Gestión de incidentes:** Gestionar los incidentes que afectan la seguridad de la información.

10. **Gestión de continuidad del negocio:** Reaccionar a la interrupción de las actividades del negocio y proteger sus procesos críticos frente a fallas, ataques o desastres.
11. **Conformidad con la legislación:** Evitar el incumplimiento de leyes, regulaciones, obligaciones y de otros requerimientos de Seguridad.

De estos once dominios se derivan los

- ***Objetivos de control,*** resultados que se esperan alcanzar mediante la implementación de controles y
- ***Los controles,*** que son las prácticas, procedimientos y/o mecanismos que reducen el nivel de riesgo.

**VENTAJAS DE LA ADOPCIÓN DE LA NORMA ISO 17799**

- Aumento de la seguridad efectiva de los sistemas de información.
- Correcta planificación y gestión de la seguridad.
- Garantías de continuidad del negocio.
- Mejora continua a través del proceso de auditoría interna.
- Incremento de los niveles de confianza de los clientes y socios de negocios.
- Aumento del valor comercial y mejora de la imagen de la organización.

**"La adopción de ISO 17799 presenta múltiples ventajas para la organización, entre ellas el primer paso para una certificación ISO 27001, pero ni la adopción de ISO 17799, ni la certificación garantizan la inmunidad de la organización frente a problemas de seguridad".**

### 4.4.6 OBJETIVOS DE CONTROL Y CONTROLES APLICALES A CAVES SA EMA.

**SELECCIÓN E IMPLEMENTACIÓN DE CONTROLES.**

- Deben tenerse en cuenta en función del costo Vs la reducción de los riesgos a un nivel aceptable y de las pérdidas que podrían producirse
- Los controles que se consideran esenciales para una organización, desde el punto de vista legal comprenden:
    - Protección de datos y confidencialidad de la información personal.
    - Protección de registros y documentos de la organización
    - Derechos de propiedad intelectual
- Los controles considerados como práctica recomendada de uso frecuente en la implementación de la seguridad de la información comprenden:
    - Documentación de la política de seguridad de la información.
    - Asignación de responsabilidades en materia de seguridad de la información.
    - Instrucción y entrenamiento en materia de seguridad de la información
    - Comunicación de incidentes relativos a la seguridad
    - Administración de la continuidad de la empresa.

***De acuerdo a los resultados de la Auditoría realizada utilizando COBIT como marco de Referencia, se puede sugerir una SELECCION de los objetivos de control y controles aplicables a CAVES SA EMA los cuales se listan con la numeración dada en el estándar ISO/IEC 17799:2005:***

- Nivel 1 (Ej.: 1 Cláusula): corresponde a las cláusulas de control de seguridad.
- Nivel 2 (Ej.: 1.1 Objetivo de control): corresponde a los objetivos de control de seguridad.
- Nivel 3 (Ej.: 1.1.1 Control): corresponde a los controles de seguridad.

## 5 POLÍTICA DE SEGURIDAD

### *5.1 Política de seguridad de la información*

5.1.1 Documento de la política de la seguridad de la información .

5.1.2 Revisión de la política de la seguridad de la información.

## 6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

### *6.1 Organización interna*

6.1.1 Compromiso de la gerencia con la seguridad de la información.

6.1.2 Coordinación de la seguridad de la información.

6.1.3 Asignación de las responsabilidades de la seguridad de la información.

6.1.4 Autorización del proceso para facilidades procesadoras de información.

6.1.5 Acuerdos de confidencialidad.

6.1.6 Contacto con las autoridades.

6.1.7 Contacto con grupos de interés especial.

6.1.8 Revisión independiente de la seguridad de la información.

***6.2 Grupos o personas externas***

6.2.1 Identificación de los riesgos relacionados con los grupos externos.

6.2.3 Tratamiento de la seguridad en acuerdos con terceros.

## 7 GESTIÓN DE ACTIVOS

***7.1 Responsabilidad por los activos***

7.1.1 Inventario de los activos.

7.1.2 Propiedad de los activos.

7.1.3 Uso aceptable de los activos.

***7.2 Clasificación de la información***

7.2.1 Lineamientos de clasificación.

7.2.2 Etiquetado y manejo de la información.

## 8 SEGURIDAD DE RECURSOS HUMANOS

***8.1 Antes del empleo***

8.1.1 Roles y responsabilidades.

8.1.2 Investigación de antecedentes.

8.1.3 Términos y condiciones del empleo.

***8.2 Durante el empleo***

8.2.1 Responsabilidades de la gerencia .

8.2.2 Conocimiento, educación y capacitación en seguridad de la información.

8.2.3 Proceso disciplinario.

***8.3 Terminación o cambio de empleo***

8.3.1 Responsabilidades de terminación.

8.3.2 Devolución de activos.

8.3.3 Retiro de los derechos de acceso.

## 9 SEGURIDAD FÍSICA Y AMBIENTAL

**9.1 Áreas seguras**

9.1.1 Perímetro de seguridad física.

9.1.2 Controles de ingreso físico.

9.1.3 Asegurar las oficinas, habitaciones y medios.

9.1.4 Protección contra amenazas externas e internas.

9.1.5 Trabajo en áreas aseguradas.

9.1.6 Áreas de acceso público, entrega y carga.

**9.2 Equipo de seguridad**

9.2.1 Ubicación y protección del equipo.

9.2.2 Servicios públicos de soporte.
9.2.3 Seguridad del cableado.
9.2.4 Mantenimiento de equipo.
9.2.5 Seguridad del equipo fuera del local.
9.2.6 Seguridad de la eliminación o re-uso del equipo.
9.2.7 Retiro de propiedad.

## 10 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

***10.1 Procedimientos y responsabilidades operacionales***

10.1.1 Procedimientos de operación documentados.
10.1.2 Gestión del cambio.
10.1.3 Segregación de los deberes.
10.1.4 Separación de los medios de desarrollo, prueba y operación.

***10.2 Gestión de la entrega del servicio de terceros***

10.2.1 Entrega del servicio.
10.2.2 Monitoreo y revisión de los servicios de terceros.
10.2.3 Manejo de cambios en los servicios de terceros.

***10.3 Planeación y aceptación del sistema***

10.3.1 Gestión de la capacidad.
10.3.2 Aceptación del sistema.

***10.4 Protección contra el código malicioso y móvil***

10.4.1 Controles contra códigos maliciosos.
10.4.2 Controles contra códigos móviles.

***10.5 Respaldo***

10.5.1 Respaldo de información.

***10.6 Gestión de seguridad de la red***

10.6.1 Controles de redes.
10.6.2 Seguridad de los servicios de la red.

**10.7 Gestión de medios**

10.7.1 Gestión de medios removibles.
10.7.2 Eliminación de medios.
10.7.3 Procedimientos para el manejo de la información.
10.7.4 Seguridad de la documentación del sistema.

***10.8 Intercambio de información***

10.8.1 Políticas y procedimientos de intercambio de información.
10.8.2 Acuerdos de intercambio.
10.8.3 Medios físicos en tránsito.
10.8.4 Mensajes electrónicos.

10.8.5 Sistemas de información comercial.

***10.9 Servicios de comercio electrónico***

10.9.1 Comercio electrónico.

10.9.2 Transacciones en línea.

10.9.3 Información públicamente disponible.

**10.10 Monitoreo**

10.10.1 Registro de auditoría.

10.10.2 Uso del sistema de monitoreo.

10.10.3 Protección del registro de información.

10.10.4 Registros del administrador y operador.

10.10.5 Registro de fallas.

10.10.6 Sincronización de relojes.

## 11 CONTROL DE ACCESO

***11.1 Requerimiento del negocio para el control de acceso***

11.1.1 Política de control de acceso.

***11.2 Gestión de acceso del usuario***

11.2.1 Registro del usuario.

11.2.2 Gestión de privilegios.

11.2.3 Gestión de las claves secretas de los usuarios.

11.2.4 Revisión de los derechos de acceso del usuario.

***11.3 Responsabilidades del usuario***

11.3.1 Uso de claves secretas.

11.3.2 Equipo desatendido de usuario.

11.3.3 Política de escritorio y pantalla limpios.

***11.4 Control de acceso a la red***

11.4.1 Política sobre el uso de los servicios de la red.

11.4.2 Autenticación del usuario para las conexiones externas.

11.4.3 Identificación del equipo en las redes.

11.4.4 Protección del puerto de diagnóstico y configuración remoto.

11.4.5 Segregación en redes.

11.4.6 Control de conexión a la red.

11.4.7 Control de routing de la red.

***11.5 Control de acceso al sistema de operación***

11.5.1 Procedimientos para un registro seguro.

11.5.2 Identificación y autenticación de usuario.

11.5.3 Sistema de gestión de claves secretas.

11.5.4 Uso de las utilidades del sistema.

11.5.5 Cierre de una sesión por inactividad.

11.5.6 Limitación de tiempo de conexión.

***11.6 Control de acceso a la aplicación e información***

11.6.1 Restricción del acceso a la información.
11.6.2 Aislar el sistema confidencial.
11.7.1 Computación y comunicaciones móviles.

### 4.4.7 ORGANIGRAMA DEL PROYECTO.


| CARGO | PERFIL | FUNCIONES |
|---|---|---|
| **Lider Proyecto** | Ing Sistemas con experiencia en proyectos medianos y manejo de personal | Administrar el Proyecto |
| **Consultor NORMA ISO 17799** | Experto Consultor con Amplios Conocimientos NORMA ISO 17799 | Dar soporte en el area |
| **Involucrado en el Negocio** | Persona con amplios conocimientos en todos los procesos del Negocio | Proporciona información acerca del nivel de riesgo que se considera aceptable. Proporciona información de históricos que sirvan de ayuda para la identificación de los riesgos del proyecto. |
| **Jefe de IT** | Ingeniero en Sistemas con conocimientos en Seguridad de la Información | Desarrolla y mantiene el plan de gestión de riesgos. Durante el proyecto debe llevar a cabo la monitorización y control de los riesgos de los que es responsable, mandar las actualizaciones de su registro al jefe de proyecto y de escalar situaciones excepcionales al jefe de proyecto |

### 4.4.8 ORGANIZACIÓN DE LOS RECURSOS.

| BIENES A ADQUIRIR PARA EL PROYECTO | |
|---|---|
| DESCRIPCION | COSTO TOTAL |
| SOFTWARE Y HARDWARE | 0,00 |
| | |
| SUBTOTAL: | 0,00 |
| TOTAL DE BIENES A ADQUIRIR: | 0,00 |

| RECURSOS HUMANOS PROPIOS QUE INTERVENDRAN EN EL PROYECTO | | | | | |
|---|---|---|---|---|---|
| NOMBRE Y APELLIDO | PROFESION U OFICIO | FUNCION EN EL PROYECTO | SUELDO MENSUAL | NUMERO DE MESES | COSTO TOTAL |
| | Ing. Sistemas | Lider de proyecto | 1.800,00 | 6 | 0,00 |
| | Ing. Sistemas | Ingeniero en Sistemas | 1.200,00 | 6 | 0,00 |
| | | Involucrado en el Negocio | 1.200,00 | 6 | 0,00 |
| | | | | | |
| TOTAL DE RECURSOS HUMANOS: | | | | | 0,00 |

| CONSULTORIA Y SERVICIOS TECNOLOGICOS A CONTRATAR | | | |
|---|---|---|---|
| DESCRIPCION | COSTO MENSUAL | NUMERO DE MESES | COSTO TOTAL |
| Consultor Experto NORMA ISO 17799 | 2.500,00 | 6 | 15.000,00 |
| Capacitación en NORMA ISO 17799 Personal IT | 2.400,00 | 1 | 2.400,00 |
| | | | |
| TOTAL DE CONSULTORIA Y SERVICIOS TECNOLOGICOS A CONTRATAR: | | | 17.400,00 |

| MATERIALES E INSUMOS | | | | |
|---|---|---|---|---|
| DETALLE | UNIDAD DE MEDIDA | CANTIDAD | COSTO UNITARIO | COSTO TOTAL |
| Papel | Resma | 10,00 | 8,00 | 80,00 |
| Toner | Cartucho | 1,00 | 90,00 | 90,00 |
| Pizarra | Unidades | 1,00 | 60,00 | 60,00 |
| Marcadores Tiza liquida | Marcador | 5,00 | 1,50 | 7,50 |
| Esferos | Unidad | 10,00 | 0,50 | 5,00 |
| | | | | 0,00 |
| **TOTAL DE MATERIALES E INSUMOS:** | | | | **242,50** |

## RESUMEN CONSOLIDADO

| DESCRIPCIONES | RESUMEN DE CUADROS | RESUMEN DE COSTOS |
|---|---|---|
| BIENES | 0,00 | 0,00 |
| RECURSOS HUMANOS | 0,00 | 0,00 |
| CONSULTORIAS Y SERVICIOS | 17.400,00 | 17.400,00 |
| MATERIALES E INSUMOS | 242,50 | 242,50 |
| TOTALES | **17.642,50** | **17.642,50** |

| **Duración del proyecto** | 6 | meses |
|---|---|---|

| COSTO TOTAL | Mes 1 al 6 | | | | | | |
|---|---|---|---|---|---|---|---|
| DESCRIPCION | 1 | 2 | 3 | 4 | 5 | 6 | TOTAL |
| BIENES DE CAPITAL | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| RECURSOS HUMANOS | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| CONSULTORIAS Y SERVICIOS | 4.900,00 | 2.500,00 | 2.500,00 | 2.500,00 | 2.500,00 | 2.500,00 | 17.400,00 |
| MATERIALES E INSUMOS | 40,42 | 40,42 | 40,42 | 40,42 | 40,42 | 40,42 | 242,50 |
| **TOTALES** | 4.940,42 | 2.540,42 | 2.540,42 | 2.540,42 | 2.540,42 | 2.540,42 | 17.642,50 |

## 4.4.9 PLANIFICACION TEMPORAL

| DESCRIPCION DE LAS ETAPAS | |
|---|---|
| CODIGO ETAPA | DESCRIPCION |
| A | ARRANQUE DEL PROYECTO |
| B | POLÍTICA DE SEGURIDAD |
| C | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN |
| D | GESTIÓN DE ACTIVOS |
| E | SEGURIDAD DE RECURSOS HUMANOS |
| F | SEGURIDAD FÍSICA Y AMBIENTAL |
| G | GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES |
| H | CONTROL DE ACCESO |

**DESCRIPCION DE LAS ACTIVIDADES DENTRO DE LA ETAPA**

| | | | MES 1 | | | | MES 2 | | | | MES 3 | | | | MES 4 | | | | MES 5 | | | | MES 6 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CODIGO ETAPA | CODIGO ACTIVIDAD | DESCRIPCION | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 |
| A | 1 | Estudio de oportunidad | | | | | | | | | | | | | | | | | | | | | | | | |
| A | 2 | Determinación del alcance del proyecto | | | | | | | | | | | | | | | | | | | | | | | | |
| A | 3 | Planificación del proyecto | | | | | | | | | | | | | | | | | | | | | | | | |
| A | 4 | Lanzamiento del proyecto | | | | | | | | | | | | | | | | | | | | | | | | |
| A | 5 | Capacitación NORMA ISO 17799 | | | | | | | | | | | | | | | | | | | | | | | | |
| B | 1 | Política de seguridad de la información | | | | | | | | | | | | | | | | | | | | | | | | |
| C | 1 | Organización interna | | | | | | | | | | | | | | | | | | | | | | | | |
| C | 2 | Grupos o personas externas | | | | | | | | | | | | | | | | | | | | | | | | |
| D | 1 | Responsabilidad por los activos | | | | | | | | | | | | | | | | | | | | | | | | |
| D | 2 | Clasificación de la información | | | | | | | | | | | | | | | | | | | | | | | | |
| E | 1 | Antes del empleo | | | | | | | | | | | | | | | | | | | | | | | | |
| E | 2 | Durante el empleo | | | | | | | | | | | | | | | | | | | | | | | | |
| E | 3 | Terminación o cambio de empleo | | | | | | | | | | | | | | | | | | | | | | | | |
| F | 1 | Áreas seguras | | | | | | | | | | | | | | | | | | | | | | | | |
| F | 2 | Equipo de seguridad | | | | | | | | | | | | | | | | | | | | | | | | |
| G | 1 | Procedimientos y responsabilidades operacionales | | | | | | | | | | | | | | | | | | | | | | | | |
| G | 2 | Gestión de la entrega del servicio de terceros | | | | | | | | | | | | | | | | | | | | | | | | |
| G | 3 | Planeación y aceptación del sistema | | | | | | | | | | | | | | | | | | | | | | | | |
| G | 4 | Protección contra el código malicioso y móvil | | | | | | | | | | | | | | | | | | | | | | | | |
| G | 5 | Respaldo | | | | | | | | | | | | | | | | | | | | | | | | |
| G | 6 | Gestión de seguridad de la red | | | | | | | | | | | | | | | | | | | | | | | | |
| G | 7 | Gestión de medios | | | | | | | | | | | | | | | | | | | | | | | | |
| G | 8 | Intercambio de información | | | | | | | | | | | | | | | | | | | | | | | | |
| G | 9 | Monitoreo | | | | | | | | | | | | | | | | | | | | | | | | |
| H | 1 | Requerimiento del negocio para el control de acceso | | | | | | | | | | | | | | | | | | | | | | | | |
| H | 2 | Gestión de acceso del usuario | | | | | | | | | | | | | | | | | | | | | | | | |
| H | 3 | Responsabilidades del usuario | | | | | | | | | | | | | | | | | | | | | | | | |
| H | 4 | Control de acceso a la red | | | | | | | | | | | | | | | | | | | | | | | | |
| H | 5 | Control de acceso al sistema de operación | | | | | | | | | | | | | | | | | | | | | | | | |
| H | 6 | Control de acceso a la aplicación e información | | | | | | | | | | | | | | | | | | | | | | | | |

## 4.5 PROYECTO 3: IMPLEMENTACION DE SYSID COMO UNA SOLUCION DE MESA DE AYUDA BASADO EN LAS MEJORES PRÁCTICAS DE ITIL

### 4.5.1 DELIMITACION

**CAMPO :** Proyecto De Inversión
**AREA :** Plan de Negocios. Tecnología
**UBICACION :** Departamento de Tecnología y Sistemas.
CAVES SA EMA, PLANTA CENTRAL
Tumbaco - Quito - Ecuador

### 4.5.2 JUSTIFICACION

De acuerdo a los resultados de la Auditoría realizada al Departamento de Sistemas utilizando COBIT como marco de Referencia , se evidenció que Departamento de TI no tiene personal asignado específicamente para el proceso de Administración de la mesa de servicio e incidentes, y además no existe herramientas automatizadas para responder a las consultas de los usuarios y para administrar la resolución de problemas. El proceso no está estandarizado y solo se proporciona soporte reactivo. No existe seguimiento a las consultas y problemas de los usuarios. No hay un proceso de jerarquización para garantizar que los problemas sean resueltos.

Aceptando la Recomendación emitida por los Auditores de requiere Implementar una Solución de Mesa de Ayuda para la empresa, con base en las mejores prácticas de ITIL.

La Mesa de Ayuda proporcionará un único punto de contacto entre los usuarios y clientes con las tecnologías de la información basado en las mejores prácticas de ITIL establecidas en los tomos de Soporte de Servicio y la Prestación del Servicio los cuales describen los procesos claves para el

manejo eficiente y efectivo de la infraestructura IT, garantizando los niveles de calidad de los servicios con la organización y sus clientes.

### 4.5.3 OBJETIVO GENERAL

Presentar una propuesta de implementación de SYSID como una Solución automatizada de Mesa de Ayuda cuyo marco de trabajo se basa en ITIL, que permita medir, verificar, controlar y retroalimentar la información para mejorar la atención a los usuarios informáticos de CAVES SA EMA.

### 4.5.4 MARCO TEORICO

#### 4.5.4.1 Objetivos de ITIL

El objetivo que persigue ITIL es diseminar las mejores prácticas en la gestión de servicios de Tecnologías de Información de forma sistemática y coherentemente. El planteo principal se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos.

ITIL está especialmente desarrollada para reducir los costos de provisión y soporte de los servicios de TI, al mismo tiempo que se garantizan los requerimientos de la información en cuanto a seguridad manteniendo e incrementando sus niveles de fiabilidad, consistencia y calidad.

#### 4.5.4.2 Los Libros de ITIL

La Biblioteca de Infraestructura de Tecnologías de Información, ITIL es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información TI. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

ITIL se considera a menudo junto con otros marcos de trabajo de mejores prácticas como la Information Services Procurement Library (ISPL, Biblioteca de adquisición de servicios de información), la Application Services Library (ASL, Biblioteca de servicios de aplicativos). El concepto de gestión de servicios de TI, aunque relacionado con ITIL, no es idéntico: ITIL contiene una sección específicamente titulada «Gestión de Servicios de TI (la combinación de los volúmenes de Servicio de Soporte y Prestación de Servicios, que son un ejemplo específico de un marco ITSM).

ITIL fue publicado como un conjunto de libros, cada uno dedicado a un área específica dentro de la Gestión de TI. Los nombres ITIL e IT Infrastructure Library (‘Biblioteca de infraestructura de TI’) son marcas registradas de la Office of Government Commerce (‘Oficina de comercio gubernamental’, OGC), que es una división del Ministerio de Hacienda del Reino Unido.

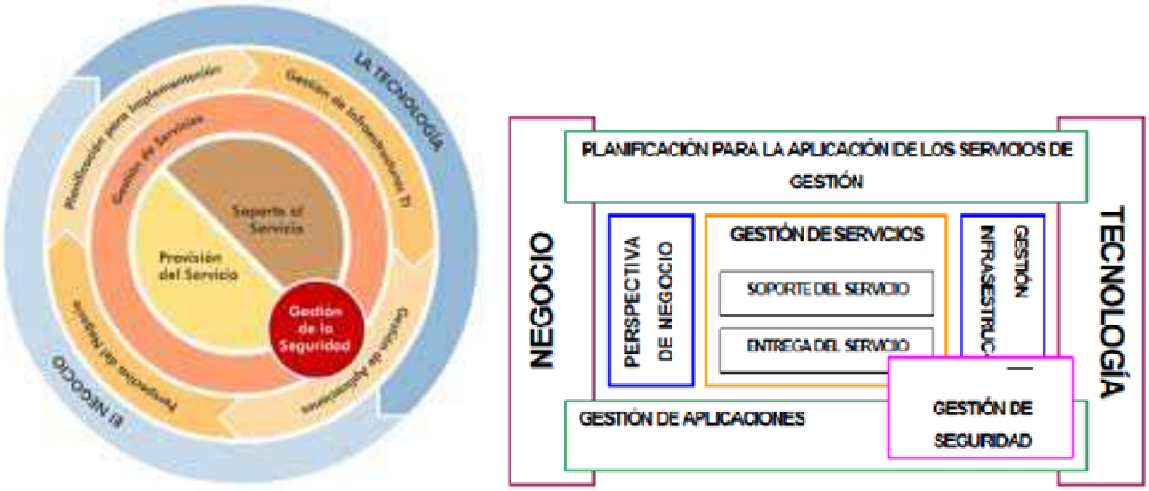



**Figura 4.3 : Contenido Libros ITIL**

En la figura se detalla el contenido de los libros de ITIL que básicamente se divide en siete partes importante:

- Planificación para la implementación de la Gestión de Servicios TI
- Gestión de Servicios
- Soporte de Servicio
- Prestación del Servicio
- Gestión de la Infraestructura
- Perspectiva del Negocio
- Gestión de la Aplicación

Estos procesos son claves para el manejo eficiente y efectivo de la infraestructura TI, garantizan los niveles de calidad de los servicios con la organización y sus clientes.

Los libros de Soporte de Servicio y Prestación de Servicio, describen los procesos claves para el manejo eficiente y efectivo de la infraestructura TI.

Garantizan los niveles de calidad de los servicios con la organización y sus clientes.

Es importante recalcar que se realiza el presente estudio tomando como base

la versión 2 de ITIL

La versión 2 se enfoca principalmente en:

- Soporte del Servicio
- Prestación de Servicios

La versión 2 de ITIL procura:

- Alinear los servicios a las necesidades presentes y futuras de la empresa y sus clientes.
- Mejorar la satisfacción del cliente.
- Mejorar la accesibilidad de los servicios a los usuarios a través de un único punto de contacto.
- Enfocar proactivamente la prestación de servicios.
- Mejorar la tasa de resolución de problemas e incidentes relacionados con las TI.
- Mejorar la utilización de los recursos.

- Mejorar la calidad y la puntualidad de las respuestas a las preguntas y quejas de los clientes.
- Mejorar el trabajo en equipo y comunicación.
- Mejorar la calidad de la información para la gestión y de apoyo a la decisión óptima.
- Mejorar la vigilancia de los resultados en relación con los compromisos de niveles de servicio SLA (Service Level Agreement)
- Mejorar la percepción de los servicios prestados.
- Aumentar la satisfacción de servicio al cliente.
- Identificar y proporcionar indicadores claves
- Reducir el costo del desarrollo de prácticas y procedimientos.
- Establecer una mejor comunicación entre el personal y los clientes.
- Mejorar el uso de los conocimientos y la experiencia para una mayor productividad.
- Fortalecer las infraestructuras
- Justificar los costes de prestación de servicios de calidad.
- Crear una infraestructura TI para la prestación de los servicios actuales y futuros de la empresa
- Mejorar la gestión y el control de las infraestructuras tecnológicas.
- Mejorar la calidad de los servicios con tal de aumentar la prestación de servicios.
- Mejorar la eficiencia y la eficacia del uso de los recursos relacionados con la prestación de servicios y potencialmente reducir los costos.

- Aplicar las mejores prácticas con respecto a la tecnología y a las necesidades empresariales actuales y futuras de su empresa.
- Mejorar la calidad de los servicios prestados a los clientes.
- Mejorar el control sobre sus servicios.
- Reducir y controlar los costos a largo plazo.

A continuación se muestra las características de los beneficios que se pueden obtener en los procesos centrales de ITIL que están explícitos en los libros de Soporte al Servicio y Entrega del Servicio.


**Figura 4.4 : Características Procesos Centrales ITIL**

### 4.5.5 ARQUITECTURA TECNOLOGICA

#### 4.5.5.1 Centro de Servicios (Mesa de Ayuda)

El objetivo principal de la Mesa de Ayuda es proveer de un punto centralizado de contacto para los usuarios que demanden de algún tipo de servicio a sus problemas informáticos, la infraestructura planteada permitirá involucrar a varios recursos locales o a terceros para la atención oportuna y efectiva a fin de retornar el servicio en el menor tiempo posible y permitir una continuidad de las operaciones, manteniendo niveles de satisfacción adecuados y acordes a la necesidad del negocio

Un centro de Servicios debe funcionar como un centro neurálgico de todos los procesos de soporte al servicio:

- Registrando y monitoreando incidentes
- Aplicando soluciones temporales a errores conocidos con la colaboración de Gestión de Problemas
- Colaborando con la Gestión de Configuraciones para asegurar la actualización de las bases de datos correspondientes.
- Gestionando cambios solicitados por los clientes mediante peticiones de servicio en colaboración con la Gestión de Cambios y de Versiones
- Soportando al negocio en la identificación de nuevas oportunidades en los contactos con usuarios y clientes.

#### 4.5.5.2 Estructuración del Servicio de Mesa de Ayuda.

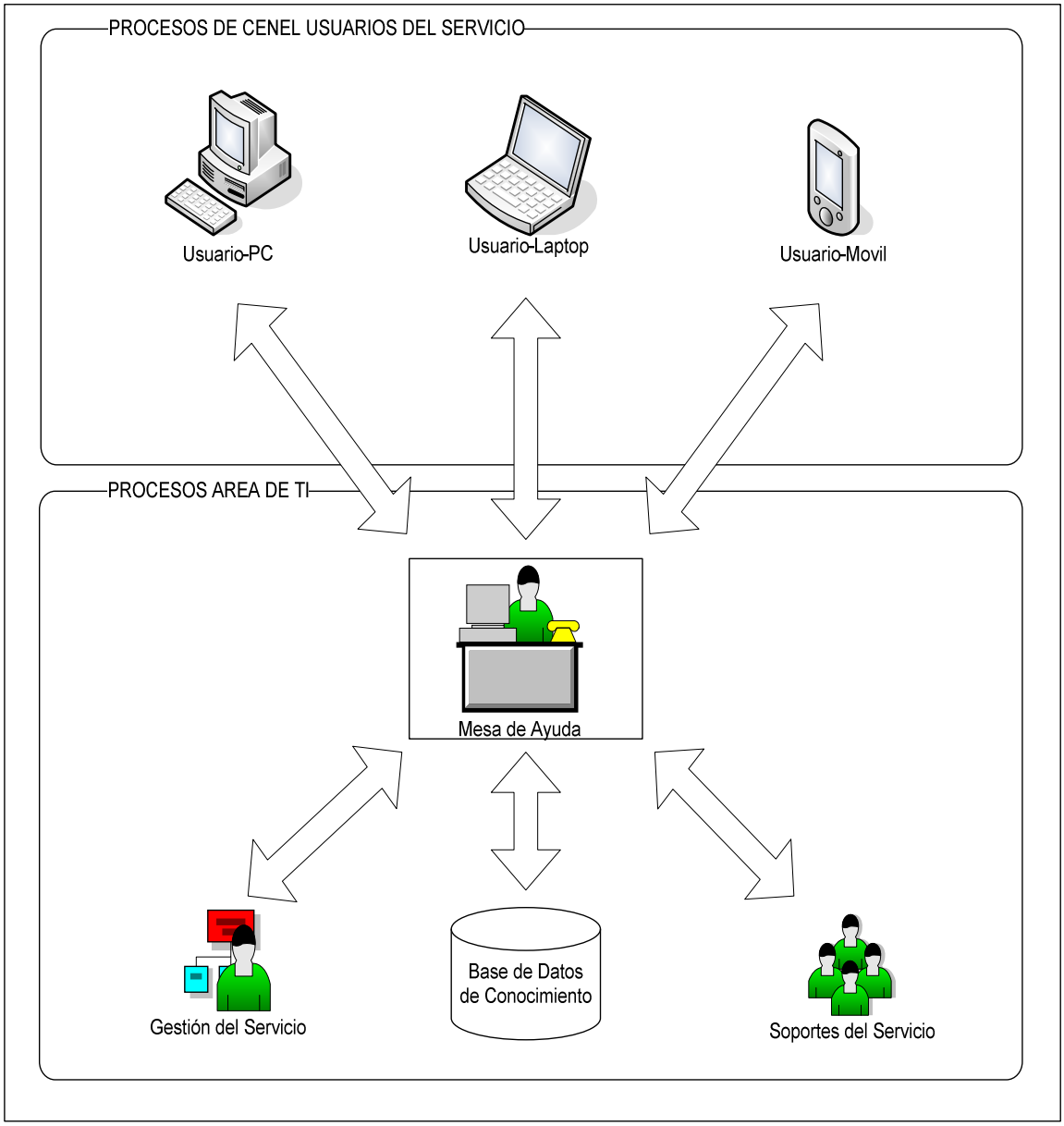



**Figura 4.5 : Arquitectura Mesa de Ayuda**

#### 4.5.5.3 Funciones Claves de la Solución

- Solución a los incidentes y/o problemas reportados por los usuarios vía telefónica (remota), y en sitio si fuere el caso.
- Asesoría y capacitación en la utilización de las aplicaciones informáticas.
- Solución de requerimientos de mantenimiento.
- Coordinación y control de cambios de infraestructura.
- Informes de seguimiento y coordinación del soporte TI.
- Medidas del servicio para los usuarios que lo requieran.
- Información a usuarios de progreso y solución de pedidos.

#### 4.5.5.4 Niveles de Escalamiento.

**Soporte de Primer Nivel:** el usuario acudirá mediante mail, llamada o en forma personal y este a su vez generará un registro y proveerá de una solución inicial, si esta llega a superar el problema se tratará de un Soporte de Primer Nivel, es decir no demandará de una especialización adicional.

**Soporte de Segundo Nivel:** Se involucrará la interrelación con un soporte más especializado que demande de conocimientos técnicos especializados para la resolución de un problema.

**Soporte de Tercer Nivel (caso especial):** soporte especializado contratado por evento, debido a que la empresa no dispone de los recursos para dar solución.

### 4.5.6 JUSTIFICACION HERRAMIENTA SOFTWARE

El momento de optar por una solución tecnológica en la actualidad ya no depende meramente de costos, sino que es una cuestión fundamental para todo directivo por las implicaciones estratégicas que pueda tener.

SysAid es una de las soluciones de Administración de TI líderes en el mercado, utilizada en más de 50.000 organizaciones y 120 países alrededor del mundo. Ofrece una simple y comprensiva solución de Mesa de Ayuda y Administración de Activos.

La herramienta **SysAid** está construida y basada en la FRAMEWORK ITIL

SYSAID es una herramienta informática que une la capacidad de realizar Inventarios dinámicos en una instalación con un potente sistema de ayuda a usuarios para la notificación, seguimiento y resolución de incidencias. Suma a estas características un sistema de control remoto de usuarios. Es ITIL complain.

#### 4.5.6.1 Beneficios

- **Solución todo en uno** : SysAid combina la ayuda de escritorio, el control remoto, la gestión de los activos, la monitorización y las herramientas de análisis de actividad, todo ello de manera sencilla.
- ***El mejor tiempo de respuesta*** Con SysAid, el departamento de Soporte Técnico, puede responder de manera más rápida y eficaz a las solicitudes - incluso a las remotas. Esto significa no sólo el ahorro de recursos, sino la mayor satisfacción del usuario final.

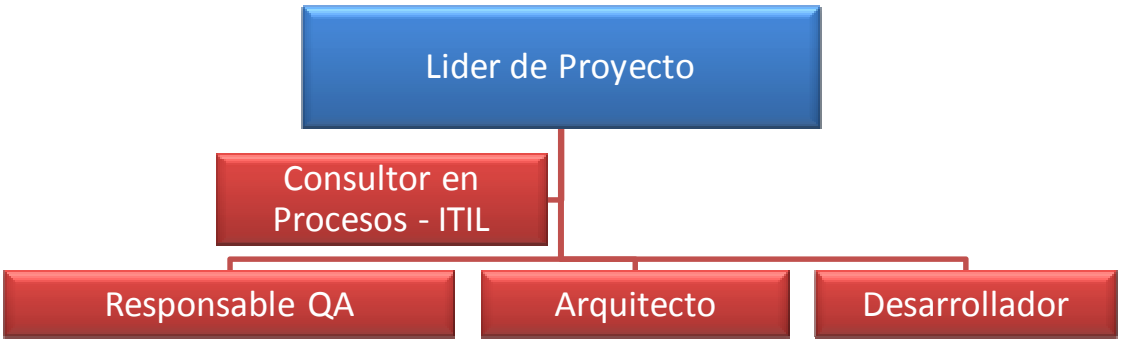
- **Incremento de la productividad IT:** SysAid aumenta la productividad IT y la disponibilidad general del sistema al reducir el tiempo dedicado al mantenimiento de la administración.
- **Mínima necesidad de recursos para la implementación e integración:** Solución Web basada en medios no costosos, el sistema puede ser instalado y puesto en funcionamiento en cuestión de horas. Estándares abiertos de servicios web XML permiten una fácil integración con los back y front-end de los sistemas

#### 4.5.6.2 Proveedores

Aunque SysAid se vende principalmente online, posee Vendedores en US, Italia, Alemania, España, Panamá y Brasil.

**http://www.sysaid.com/**

### 4.5.7 ORGANIGRAMA DEL PROYECTO.




| CARGO | PERFIL | FUNCIONES |
|---|---|---|
| **Lider Proyecto** | Ing Sistemas con experiencia en proyectos medianos y manejo de personal | Administrar el Proyecto |
| **Consultor en Procesos** | Consultor con Amplios Conocimientos en Procesos | Dar soporte en el area |
| **Responsable QA** | Ing. Sistemas con experiencia en las áreas de QA y Pruebas | Responsable de la Calidad, Planificacion de pruebas de carga y planes de pruebas |
| **Arquitecto** | Ing. Sistemas con experiencia en Implementación de Soluciones Web | Generar los requisitos del sistema basado en los procesos definidos y las necesidades del usuario |
| **Desarrollador** | Analista de sistemas con conocimiento Linux y Base de Datos | Implementación de la Herramienta en base especificaciones del Arquitecto |

### 4.5.8 BIENES A ADQUIRIR PARA EL PROYECTO

| Organización de Recursos | |
|---|---|
| | |
| **BIENES A ADQUIRIR PARA EL PROYECTO** | |
| **EQUIPOS** | |
| **DESCRIPCION** | **COSTO TOTAL** |
| 1 Server HP DL380G7 E5640 Base US Svr, (1) Intel® Xeon® Processor | 0.00 |
| | |
| **SUBTOTAL:** | **0.00** |
| **INFRAESTRUCTURA FISICA Y TELECOMUNICACIONES** | |
| **DESCRIPCION** | **COSTO TOTAL** |
| Enlace de internet 4 meses | 2,600.00 |
| | |
| | |
| **SUBTOTAL:** | |
| **SOFTWARE** | |
| **DESCRIPCION** | **COSTO TOTAL** |
| SysAid Pro Edition, Cloud platform | 5,000.00 |
| | |
| **SUBTOTAL:** | **5,000.00** |
| **TOTAL DE BIENES A ADQUIRIR:** | **7,600.00** |

## 4.5.9 ORGANIZACIÓN DE LOS RECURSOS.

| RECURSOS HUMANOS PROPIOS QUE INTERVENDRAN EN EL PROYECTO | | | | | |
|---|---|---|---|---|---|
| NOMBRE Y APELLIDO | PROFESION U OFICIO | FUNCION EN EL PROYECTO | SUELDO MENSUAL | NUMERO DE MESES | COSTO TOTAL |
| | Ing. Sistemas | Lider de proyecto | 1,800.00 | 4 | 7,200.00 |
| | Ing. Sistemas | Ing QA | 1,200.00 | 1 | 1,200.00 |
| | Ing. Sistemas | Arquitecto | 1,200.00 | 2 | 2,400.00 |
| | Ing. Sistemas | Desarrollador | 950.00 | 3 | 2,850.00 |
| | | | | | 0.00 |
| | | | | SUBTOTAL: | 13,650.00 |

| CONSULTORIA Y SERVICIOS TECNOLOGICOS A CONTRATAR | | | |
|---|---|---|---|
| DESCRIPCION | COSTO MENSUAL | NUMERO DE MESES | COSTO TOTAL |
| Consultor Experto ITIL | 1,500.00 | 2 | 3,000.00 |
| | | | |
| TOTAL DE CONSULTORIA Y SERVICIOS TECNOLOGICOS A CONTRATAR: | | | 3,000.00 |

| MATERIALES E INSUMOS | | | | |
|---|---|---|---|---|
| DETALLE | UNIDAD DE MEDIDA | CANTIDAD | COSTO UNITARIO | COSTO TOTAL |
| Papel | Resma | 5.00 | 8.00 | 40.00 |
| Toner | Cartucho | 1.00 | 90.00 | 90.00 |
| Pizarra | Unidades | 1.00 | 60.00 | 60.00 |
| Marcadores Tiza liquida | Marcador | 5.00 | 1.50 | 7.50 |
| Scanner | Unidad | 1.00 | 200.00 | 200.00 |
| Esferos | Unidad | 10.00 | 0.50 | 5.00 |
| | | | | 0.00 |
| | | | | 0.00 |
| TOTAL DE MATERIALES E INSUMOS: | | | | 402.50 |

| RESUMEN CONSOLIDADO | | |
|---|---|---|
| DESCRIPCIONES | RESUMEN DE CUADROS | RESUMEN DE COSTOS |
| BIENES | 7.600,00 | 7.600,00 |
| RECURSOS HUMANOS | 0,00 | 0,00 |
| CONSULTORIAS Y SERVICIOS | 3.000,00 | 3.000,00 |
| MATERIALES E INSUMOS | 402,50 | 402,50 |
| **TOTALES** | **11.002,50** | **11.002,50** |

| **Duración del proyecto** | 4 | meses |
|---|---|---|

| COSTO TOTAL | Mes 1 al 4 | | | | | | |
|---|---|---|---|---|---|---|---|
| DESCRIPCION | 1 | 2 | 3 | 4 | | | TOTAL |
| BIENES DE CAPITAL | 1.900,00 | 1.900,00 | 1.900,00 | 1.900,00 | | | 7.600,00 |
| RECURSOS HUMANOS | 0,00 | 0,00 | 0,00 | 0,00 | | | 0,00 |
| CONSULTORIAS Y SERVICIOS | 1.500,00 | 1.500,00 | | | | | 3.000,00 |
| MATERIALES E INSUMOS | 100,63 | 100,63 | 100,63 | 100,63 | | | 402,50 |
| **TOTALES** | **3.500,63** | **3.500,63** | **2.000,63** | **2.000,63** | | | **11.002,50** |

## 4.6.0 PLANIFICACION TEMPORAL.

| DESCRIPCION DE LAS ETAPAS | |
|---|---|
| CODIGO ETAPA | DESCRIPCION |
| A | Arranque del Proyecto |
| B | Análisis de Requerimientos |
| C | Diseño de alto y bajo Nivel |
| D | Pruebas de Usuario |
| E | Entrega de la Solución |
| F | Cierre del Proyecto |

| DESCRIPCION DE LAS ACTIVIDADES DENTRO DE LA ETAPA | | | MES 1 | | | | MES 2 | | | | MES 3 | | | | MES 4 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CODIGO ETAPA | CODIGO ACTIVIDAD | DESCRIPCION | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 |
| A | 1 | Definir necesidades del cliente | | | | | | | | | | | | | | | | |
| A | 2 | Determinar el alcance de la solución | | | | | | | | | | | | | | | | |
| A | 3 | Firma de acuerdo contractual con los interesados | | | | | | | | | | | | | | | | |
| A | 4 | Preparación de cronograma | | | | | | | | | | | | | | | | |
| B | 1 | Análisis de necesidades e identificación del problema | | | | | | | | | | | | | | | | |
| B | 2 | Definición de Riesgos potenciales | | | | | | | | | | | | | | | | |
| B | 3 | Definiciones de necesidades no funcionales | | | | | | | | | | | | | | | | |
| B | 4 | Entrega final de documento detallado de necesidades al cliente | | | | | | | | | | | | | | | | |
| C | 1 | Definición de especificaciones Funcionales | | | | | | | | | | | | | | | | |
| C | 2 | Levantamiento de requerimientos | | | | | | | | | | | | | | | | |
| C | 3 | Definición de Especificaciones Técnicas | | | | | | | | | | | | | | | | |
| C | 4 | Diseño del Portal Web | | | | | | | | | | | | | | | | |
| C | 5 | Definición de estándares | | | | | | | | | | | | | | | | |
| C | 6 | Definición de Estrategia de Pruebas | | | | | | | | | | | | | | | | |
| C | 7 | Definición de Plan de Pruebas | | | | | | | | | | | | | | | | |
| C | 8 | Definición de Riesgos y plan de contingencia | | | | | | | | | | | | | | | | |
| D | 1 | Instalación y configuración en ambiente de TEST | | | | | | | | | | | | | | | | |
| D | 2 | Ejecución pruebas Funcionales | | | | | | | | | | | | | | | | |
| D | 3 | Corrección de problemas en pruebas funcionales | | | | | | | | | | | | | | | | |
| D | 4 | Ejecución pruebas Funcionales por usuario experto | | | | | | | | | | | | | | | | |
| D | 5 | Corrección de problemas con usuario experto | | | | | | | | | | | | | | | | |
| D | 6 | Ejecución pruebas Técnicas | | | | | | | | | | | | | | | | |
| D | 7 | Corrección de problemas en pruebas técnicas | | | | | | | | | | | | | | | | |
| D | 8 | Elaboración de Informe final de ejecución de pruebas | | | | | | | | | | | | | | | | |
| D | 9 | Preparación de Capacitación para equipo de producción y Usuarios Finales | | | | | | | | | | | | | | | | |
| D | 10 | Capacitar equipo de producción y Usuarios finales | | | | | | | | | | | | | | | | |
| E | 1 | Instalación y configuración en ambiente de Producción | | | | | | | | | | | | | | | | |
| E | 2 | Soporte Periodo PostImplantación | | | | | | | | | | | | | | | | |
| E | 3 | Certificación de solución en producción | | | | | | | | | | | | | | | | |
| E | 4 | Informe final de entrega del proyecto | | | | | | | | | | | | | | | | |
| F | 1 | Realizar Encuesta de satisfacción al cliente | | | | | | | | | | | | | | | | |
| F | 2 | Reporte Cierre y entrega de Documentación | | | | | | | | | | | | | | | | |
| F | 3 | Cierre formal del proyecto (carta de finiquito) | | | | | | | | | | | | | | | | |

## 4.6. CONTROL DE COSTOS PROYECTOS

| GASTOS INTERNOS | GASTOS EXTERNOS |
| --- | --- |
| • Los recursos necesarios deben ser solicitados con anticipación<br>• El recurso humano que trabaje dentro de la institución deberá reportar claramente las horas reportadas dentro de su horario de trabajo.<br>• El Software empleado en el proyecto debe ser inventariado totalmente con el fin de calcular completamente el uso de estas en el proyecto.<br>• Los utilices de oficina deben ser solicitados a Administración, llenando un formulario de recepción detallando lo entregado al proyecto. | • Facturas. Aprobadas y aceptadas por el equipo de proyecto y el Departamento Financiero. Controlando que estas se ajusten al presupuesto aprobado y establecido para el proyecto<br>• Cada una de estas facturas deberá estar relacionada directamente con una fase del proyecto, con la finalidad de tener una visión clara del gasto y su propósito.<br>• No se debe permitir que la adquisición de los productos o servicios externos dilaten o retrasen actividades del proyecto, es decir, deben tener bien definidas las fechas de entrega. Caso contrario si se entregasen fuera del plazo se deberá definir penalización sobre esta entrega del producto servicio. |

## 4.7 SEGUIMIENTO Y CONTROL PROYECTOS

| Etapa | Entregable |
|---|---|
| **Inicio del proyecto** | Contrato firmado y entregado |
| **Elaboración del Presupuesto** | Presupuesto firmado y acordado |
| **Aprobación del Presupuesto** | Aprobación del presupuesto |
| **Firma de Contratos** | Aceptación del Contrato |
| **Arranque del proyecto** | Acta de inicio formal del proyecto firmada por los áreas |
| **Análisis de Requerimientos** | Documento de Visión, Misión y necesidades del proyecto aprobado y firmado por el Cliente |
| **Diseño Sistema** | Documento de Especificaciones Funcionales |
| **Desarrollo y Pruebas Unitarias** | Documento de Especificaciones Técnicas |
| **Pruebas del sistema / certificación** | Estrategia de pruebas |
| | Guiones de pruebas |
| | Certificación de pruebas unitarias |
| | Certificación de pruebas del Sistemas |
| | Manual de instalación e implantación |
| | Certificación de pruebas funcióneles |
| | Certificación de pruebas técnicas |
| | Certificación por parte del usuario experto |
| | Manual de usuario |
| | Manual de operación |
| **Implementación en producción** | Solución puesta en producción |
| **Soporte Post Implementación** | OK del Cliente de aceptación de la solución en |
| **Cierre del Proyecto** | Encuesta de Satisfacción |
| | Acta de finiquito del proyecto |

## 4.8 RESUMEN EJECUTIVO PROYECTOS

| RECURSOS | PROYECTO 1<br>Implementación de Magerit como una Solución para Análisis y Gestion de Riesgos | PROYECTO 2<br>Elaboración de un Plan de Seguridad basado en la Norma ISO/IEC 17799:2005 | PROYECTO 3<br>Implementación de SYSID como una Solución de Mesa de Ayuda basado en la Mejores Prácticas ITIL | TOTAL |
|---|---|---|---|---|
| BIENES | 2,456.10 | | 7,600.00 | 10,056.10 |
| RECURSOS HUMANOS (COSTO INCREMENTAL) | 14,400.00 | 25,200.00 | 13,650.00 | 53,250.00 |
| CONSULTORIAS Y SERVICIOS | 5,200.00 | 17,400.00 | 3,000.00 | 25,600.00 |
| MATERIALES E INSUMOS | 402.50 | 242.50 | 402.50 | 1,047.50 |
| **TOTALES** | **22,458.60** | **42,842.50** | **24,652.50** | **$ 89,953.60** |
| | | | **TOTALES (Sin Costo Incremental)** | **$ 36,703.60** |
| **TIEMPO EJECUCION PROYECTOS** | 4 MESES | 6 MESES | 4 MESES | **14 MESES** |

# CAPITULO 5

## *5.1* CONCLUSIONES

- El Control Interno es una herramienta fundamental para lograr la eficiencia, eficacia, productividad y el desarrollo operativo y administrativo de las Empresas, bajo un ambiente de prevención de riesgos y pro actividad en el logro de los objetivos institucionales.
- La administración del riesgo tecnológico es un aspecto fundamental dentro de la gestión de riesgo informáticos y es una de las responsabilidades y desafíos más importantes a las cuales se enfrentan las Empresas en el Ecuador, debido a que involucra el uso de recursos organizacionales, humanos, financieros y tecnológicos
- Existen en la actualidad una serie de lineamientos, estándares y mejores prácticas para una efectiva administración del riesgo, la entrega de servicios y la seguridad relacionada con la tecnología de información, entre los que se encuentran: COBIT, ISO 27001, ITIL, entre otros.
- Es posible crear un marco de control integral para la administración del riesgo tecnológico en las PYMES, basado en mejores prácticas propuesto por , COBIT, e ISO 17799 que garantice la seguridad de la información, la salvaguarda de los recursos tecnológicos y la continuidad del negocio.

- El rol de auditoría ha evolucionado en los últimos años de tal forma que se ha convertido en un factor importante dentro de la evaluación del riesgo tecnológico y en la mejora continua de los procesos de TI, a través del uso de herramientas tecnológicas para el análisis de las operaciones, la evaluación de riesgos y la planificación de la auditoría.
- En la actualidad toda organización exitosa se ha concientizado de la importancia del manejo de las tecnologías de información (TI), especialmente en la implementación de nuevos proyectos tecnológicos que incluye costos y beneficios, pero que mejora la producción y competitividad.
- La implementación de Proyectos , Metodologías y Herramientas de Software que permitan el Análisis y Gestión de Riesgos aplicada a la infraestructura de la empresa permitirá disminuir la Brecha del Nivel de Madurez actual en relación con el Nivel Objetivo, definido en los resultados de la Auditoría Realizada.

## *5.2* RECOMENDACIONES

- La ejecución de los Proyectos de Inversión planteados se presenta como una oportunidad para lograr los objetivos institucionales; agregar valor a sus líneas de negocio y estructuras organizacionales; alcanzar una ventaja competitiva frente a la competencia; y, garantizar en forma sustentable su desarrollo administrativo, operativo, financiero y tecnológico.

- La Administración del riesgo tecnológico permitirá a la empresa hacer frente a diversos eventos y escenarios de riesgo que pudieran poner en peligro la continuidad operativa del negocio; y para ello, es necesaria la participación de toda la organización y el apoyo fundamental de la Gerencia General en la definición y formalización de las políticas de seguridad y en la implementación de un adecuado control interno de la tecnología de información.
- Se recomienda documentar todos los procesos de TI en forma gráfica y escrita, para establecer controles de seguridad de la información y de esta manera evitar que la misma sea vulnerable ante errores, fallas, etc. Además CAVES SA EMA debe tener un Plan Estratégico actualizado que sirva como guía y ayuda al Departamento de Sistemas, y este pueda elaborar su propio Plan Estratégico conjuntamente ligado al general.

# BIBLIOGRAFIA


CAVES SA EMA. (2011). *CAVES SA EMA - Servicios de Catering y Afines*. Recuperado el Enero de 2011, de www.caves-ghl.com.ec

Electrónica, P. d. (s.f.). *PAe - Portal Administración Electónica*. Recuperado el Marzo de 2012, de MAGERIT 2.0: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P80029225 1293651550991&langPae=es&detalleLista=PAE_1276529683497133

Instituto, I. G. (2007). *Cobit 4.1.*

ISACA. (2011). *http://www.isaca.org/cobit/pages/default.aspx*. Recuperado el Marzo de 2011, de ISACA, Trust In, and value from, information system: http://www.isaca.org/cobit/pages/default.aspx

IT GOVERNANCE INSTITUTE. (2007). COBIT 4.1. En *COBIT 4.1* (pág. 196).

IT GOVERNANCE INSTITUTE. (2011). *IT GOVERNANCE INSTITUTE*. Retrieved Diciembre 2011, from http://www.itgi.org/

Ltd, A. G. (2007-2012). *Official Site ITIL*. Retrieved Abril 2012, from http://www.itil-officialsite.com/

PMI - Proyect Management Institute. (2008). *GUÍA DE LOS FUNDAMENTOS PARA LA DIRECCIÓN DE PROYECTOS.* PMI Publications.

# GLOSARIO

## Glosario de términos

**Activo de información:** Cualquier información valiosa o necesaria para que la Organización cumpla sus objetivos.

**Acuerdo de nivel de servicio (SLA):** Acuerdo entre dos partes en relación a las características mínimas exigibles a un servicio prestado entre ellas.

**Amenaza:** Causa potencial de un incidente que puede resultar en un daño a un sistema o a una organización.

**Análisis de riesgos:** Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización (MAGERIT).

**Auditoría:** Examen objetivo, sistemático, profesional e independiente, aplicado a una organización por un auditor competente.

**Balanced ScoreCard:** BSC- Una herramienta de gestión que traduce la estrategia de la empresa en un conjunto coherente de indicadores.

**Benchmarking:** Proceso sistemático y continuo para evaluar comparativamente los productos, servicios y procesos de trabajo en organizaciones.

**Evaluar:** Valorar, estimar el valor de las cosas o situaciones.

**Evidencia:** Constituye en el soporte y respaldo a las afirmaciones dadas.

**Gestión de riesgos:** Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

**Gobierno :** Sistema de alta gerencia para asegurar la consecución de los objetivos de una organización.

**KGI:** Indicador clave de meta. Definen las medidas que indican a la administración - después del hecho- si un proceso de TI ha satisfecho sus requerimientos de negocio.

**KPI:** Indicador clave de desempeño. Define mediada para determinar que también se está desempeñando el proceso de TI para permitir que se alcance el objetivo; son indicadores guía de que un objetivo probablemente se alcanzará o no; y son buenos indicadores de capacidades, prácticas y habilidades.

**Implantar:** Establecer y poner en ejecución doctrinas nuevas, prácticas o costumbres.

**Mapa de riesgos:** Relación de las amenazas valoradas a las que están expuestos los activos.

**Outsourcing:** Subcontratación, el contrato que una empresa realiza a otra para que realice determinadas tareas que, originalmente, fueron asignadas a la primera.

**Política de seguridad:** Conjunto de reglas, directivas y prácticas que gobiernan cómo se gestionan, protegen los activos y recursos de información.

**Ponderar:** Pesar, determinar el peso de una cosa. Examinar con atención las razones de una cosa para formar un juicio de ella.

**Riesgo:** Estimación del grado de exposición a que una amenaza se materialice

sobre uno o más activos causando daños o perjuicios a la Organización.

**Salvaguarda:** o medida de seguridad es cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto en la organización.

**Seguridad informática:** Capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que pueden causar un daño a los recursos de información tecnológicos de una organización.

**Stakeholders:** Grupos o Individuos que pueden afectar o son afectados por las actividades de una empresa.

**Verificar:** Probar que es verdad una cosa que se duda. La auditoría es un examen que verifica y evalúa determinadas áreas de una empresa.

## GLOSARIO DE ABREVIATURAS

**AGR:** Análisis y Gestión de Riesgos

**COBIT:** Control Objectives for Information and related Technology (Objetivos de Control para tecnología de la información y relacionada).

**COSO**: Committee Of Sponsoring Organizations (Comité de organizaciones patrocinadoras de la comisión Treadway).

**ITIL:** Information Technology Infrastructure Library (Biblioteca de Infraestructura de Tecnologías de la Información.)

**ISO:** Organización Internacional de Estandarización.

**TI:** Tecnologías de la Información.