ESCUELA POLITÉCNICA DEL EJÉRCITO

DPTO. DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"EVALUACIÓN TÉCNICA INFORMÁTICA DEL COMIL 10 ABDÓN CALDERÓN, UTILIZANDO EL ESTÁNDAR INTERNACIONAL COBIT"

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR: **JOHN ALEXIS NARVÁEZ MEJÍA**

SANGOLQUÍ, Octubre del 2012

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. John Alexis Narváez Mejía como requerimiento parcial a la obtención del título de INGENIERO EN SISTEMAS E INFORMÁTICA.

01 de Octubre del 2012.

_____

Ing. Mario Ron.
Profesor Director.

AUTORIZACIÓN

Yo, John Alexis Narváez Mejía autorizo a la ESCUELA POLITÉCNICA DEL EJÉRCITO, la publicación en la Biblioteca de la Institución, la Tesis titulada "Evaluación Técnica Informática del COMIL 10 Abdón Calderón, utilizando el Estándar Internacional COBIT", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

01 de Octubre del 2012.

_____

John Narváez Mejía

. Autor.

DEDICATORIA

“Las únicas limitaciones son aquellas que nos imponemos” (Nicholas Murray Butler).

El conocimiento hace a las personas más libres, críticos y responsables. Dedico este trabajo a mi Padre que esta en el Cielo y a todas las personas que en mí influyeron, que sin tenerlo todo luchan por sus sueños y tienen deseos de triunfar, siguen sus ideas e intentan lo difícil para triunfar en la vida.

John Narváez Mejía

AGRADECIMIENTOS

Todo lo que haces hoy, es parte de la gran vida que te estás construyendo. Agradezco a mi Madre Teresa Mejía, quien me dio la vida y que con su amor y cariño me impulso a dar lo mejor de mí a lo largo de mi vida. A mi hermano Mauricio y a todos mis amigos y familiares que me brindaron su apoyo y paciencia en momentos difíciles.

Mi mas sincero agradecimiento al Ingeniero Mario Ron, por su acertada y desinteresada asesoría, durante la elaboración de este proyecto, por su comprensión y su gran profesionalismo que permitieron que concluya satisfactoriamente el presente trabajo.

Al Ing. Vinicio Cantuña integrante del Centro de Informática del COMIL Nº 10 que mostró su apoyo en todas las etapas de este proyecto.

Finalmente agradezco a mi esfuerzo y sacrificio que fueron primordiales para lograr la culminación de esta meta.

John Narváez Mejía

ÍNDICE DE CONTENIDO

LISTADO DE TABLAS

LISTADO DE CUADROS

LISTADO DE FIGURAS

LISTADO DE ANEXOS CD

ANEXOS

ANEXO A

A.1 Cuadro Resumen de la Evaluación Informática del COMIL Nº 10

ANEXO B

B.1 Entrevistas

B.2 Encuesta

ANEXO C

CARTA DE AUSPICIO

CARTA DE ACEPTACIÓN

NOMENCLATURA UTILIZADA

AI: Adquisición e Implementación.

ANS: Acuerdo de Nivel de servicio.

BD: Base de Datos.

BS: British Standard / Norma Británica.

CDI: Comando de Educación y Doctrina del Ejército Ecuatoriano.

CISA: Certified Information Systems Auditor / Certificación de Auditoría de Sistemas de Información.

COBIT: Control Objectives for Information and related Technology / Control de Objetivos para Información y Tecnología relacionada, ISACA.

COMIL: Colegio Militar Nº 10 “Abdón Calderón”

COSO: Committee of Sponsoring Organizations / Comité de Organizaciones Patrocinadoras.

DS: Entrega y Soporte.

EGB: Educación General Básica.

FDD: Feature Driven Development / Desarrollo Guiado por la Funcionalidad.

IEC: Comisión Electrotécnica Internacional.

ISACA: Information Systems Audit and Control Association / Asociación de Control y Auditoría de Sistemas de Información.

ISO: International Organization for Standardization / Organización Internacional de Normalización.

ITIL: Information Technology Infrastructure Library / Biblioteca de Infraestructura de Tecnologías de Información.

KARDEX: Herramienta para el control de inventarios.

ME: Monitorear y Evaluar.

NYSE: Bolsa de valores de Nueva York

P: Primario.

PCAOB: Public Company Accounting Oversight Board / Comisión encargada de supervisar las auditorías de las compañías que cotizan en bolsa.

PMBOK: Project Management Body of Knowledge / Cuerpo de conocimientos de la Dirección de Proyectos.

PO: Planeación y Organización.

PYMES: Pequeña y Mediana Empresa.

QA: Quality Assurance / Aseguramiento de la Calidad.

RUP: Rational Unified Process / Proceso Unificado de Rational.

S: Secundario.

SEI: Secciones Informáticas.

SENPLADES: Secretaría Nacional de Planificación y Desarrollo.

SGSI: Sistema de Gestión de la Información.

SIE: Sistema Integrado Educativo.

SIFTE: Sistema Integrado de la Fuerza Terrestre.

SLA: Service Level Agreement / Acuerdo de nivel de servicio.

SOP: Standard operating procedure / Procedimientos estándar de operaciones.

SOX: Ley Sarbanes-Oxley

TI / IT: Tecnologías de la Información

TIC: Tecnologías de Información y la Comunicación

XP: eXtreme Programming / Programación Extrema.

RESUMEN

En el presente proyecto se realizó la Evaluación Técnica Informática del Colegio Militar Nº 10 ABDÓN CALDERÓN utilizando el estándar internacional COBIT (Objetivos de Control para la Información y Tecnologías).

Los procedimientos de la gestión tecnológica que aplica actualmente el Departamento de Tecnología de Información del COMIL Nº 10, resultado de la evaluación son seleccionados y adaptados a un modelo de gestión de TI que dificulta la toma de decisiones en cuanto al desempeño de tecnologías en el interior de la Institución, además se requiere medir y controlar el desarrollo y aplicación de los procesos tecnológicos para que permitan mejorar la trayectoria estratégica y operativa.

Se presenta un reporte condensado de dicha evaluación, se identificó los factores críticos y riesgos que son obstáculo para una adecuada gestión tecnológica comprendida en la identificación de requerimientos de información relevantes para la Institución, detallando los riesgos que actualmente identifica TI, seleccionando los procesos y controles a auditar, además se facilitó instrucciones clave y controles que deben efectuarse en el Departamento Informático y se culminó con un informe final que incluye los principales hallazgos encontrados y conclusiones y recomendaciones como parte de la evaluación.

ABSTRACT

This project was the Technical Evaluation of Military College Computing No. 10 Abdon Calderon using the international standard COBIT (Control Objectives for Information and Technology).

The procedures for managing technology currently applied by the Department of Information Technology of the COMIL Nº. 10, the result of the evaluation are selected and adapted to a model of IT management that makes decisions regarding the performance of technologies within the institution also is required to measure and control the development and application of technological processes to improve its strategic and operational.

We present a condensed report of this evaluation, we identified the critical factors and risks that have hindered a proper understanding technology management in identifying information requirements relevant to the organization, detailing the risks currently identified IT processes and controls by selecting audited, as well instructions were provided key checks to be conducted in the IT Department and culminated with a final report that includes the main findings and conclusions and recommendations as part of the evaluation.

CAPÍTULO 1

GENERALIDADES

1.1 Introducción

Los Sistemas Informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los Sistemas de Información de la empresa. La Informática está subsumida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, sometidos a los generales de la misma. El Colegio Militar Nº 10 “Abdón Calderón” es una Institución pública, perteneciente al Comando de Educación y Doctrina de la Fuerza Terrestre, ante la necesidad de contar con un adecuado marco de administración y control, el COMIL Nº 10 requiere los procedimientos Informáticos de evaluación para los Sistemas de Información de la Institución y determinar falencias actuales.

La Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma y debido a su importancia en el funcionamiento de una empresa, existe la Auditoría Informática. Por tanto, el propósito a alcanzar por una organización que contrata la auditoría es asegurar que sus objetivos estratégicos son los mismos que los de la propia organización y que los sistemas prestan el apoyo adecuado a la consecución de estos objetivos, tanto en el presente como en su evolución futura. Por ser una Institución educativa, que brinda servicios de alta calidad, cuenta con una unidad de sistemas que centraliza la información para la administración,

gestión de actividades TI, desarrollo e implementación de sistemas requeridos por la Institución y se preocupa por el adecuado funcionamiento de las aplicaciones existentes, bases de datos, redes y comunicaciones, debido a ello se ha considerado la necesidad de realizar una Evaluación Técnica Informática Externa, a los controles establecidos por la gerencia de TI, bajo los estándares de un marco referencial a nivel mundial como es COBIT[1].

COBIT define las actividades de TI de una organización, mediante un modelo genérico de procesos en cuatro dominios que son: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar; lo que brinda un marco de trabajo para la medición y monitoreo del desempeño de las Tecnologías de Información, e integra las mejores prácticas administrativas.

1.2 Problema

1.2.1 Planteamiento del Problema

El establecimiento COMIL Nº 10 tiene el Departamento de Informática con oficinas equipadas, sistemas de comunicación, redes locales y algunos componentes de la tecnología y como objetivos de la automatización el mejorar los tiempos de respuesta de sus sistemas y mantener una información integra.

El sistema informático actual del establecimiento tiene seis años de uso junto con la base de datos y el tiempo de respuesta de estos sistemas no han satisfecho a los usuarios que han tenido dificultades en las gestiones

[1] **COBIT** – *Control Objectives for Information and related Technology, ISACA.*

realizadas diariamente y de este modo surgió la necesidad de una Auditoría externa al Departamento Informático. El sistema computacional es manejado por el Jefe de Sistemas y poseen un equipo de trabajo con profesionales debidamente capacitados para el monitoreo y soporte. El presupuesto que se asigna al equipo informático se lo hace de acuerdo a las necesidades planteadas por el Jefe de Sistemas y durante el año si existiera un daño de hardware se invierte en este rubro, para lo que implica mejoramiento del software no existe un plan realizado o presupuesto asignado.

El COMIL Nº 10 tiene un incremento constante de las expectativas y necesidades relacionadas con la auditoría informática externa, al igual que la actualización continua de los elementos que componen la tecnología, obligándola a requerir controles, realizar evaluaciones periódicas y completas de los sistemas de información a cargo de personal calificado.

Desde el punto de vista del nivel de Dirección de la Institución, el Departamento de Informática y los sistemas informáticos se encuentran funcionando de manera adecuada, pero hasta la actualidad no se ha realizado ninguna auditoría que pueda verificar e informar sobre el real y correcto funcionamiento del Departamento de Informática.

1.3 Interrogantes de la Evaluación Técnica Informática

1.3.1 Pregunta General

¿Cuál es el Objetivo principal de la auditoría informática?

Es emitir una opinión acerca de la eficiencia en la adquisición y utilización de los recursos informáticos, la confiabilidad, integridad, seguridad y

oportunidad de la información y la efectividad de los controles en los sistemas de información.

1.3.2 Preguntas Específicas

¿Cuál es el objetivo de COBIT en una Auditoría Informática?

El objetivo COBIT es investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para TI que sean autorizados, actualizados, e internacionales para el uso del día a día de los gestores de negocios y auditores.

¿Cómo me puede ayudar COBIT en la Auditoría Informática?

Gestores, auditores, y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de TI que ayuda a la adecuada toma de decisiones a nivel de Dirección de Tecnología.

¿Cómo se mejora la administración con la Auditoría Informática?

- Asegurar la ética en la administración, por medio de un eficiente control posterior.
- Verificar la confiabilidad, oportunidad y pertinencia de la información financiera y administrativa.
- Poner de manifiesto y corregir las irregularidades, errores, desviaciones o deficiencias de las operaciones.
- Evaluar los sistemas de control interno y formular recomendaciones para mejorarlos.

1.4 Objetivos

1.4.1 Objetivo General

- Realizar una auditoría informática del Sistema de Información del COMIL Nº 10 ABDÓN CALDERÓN utilizando el Estándar Internacional Objetivos de Control para la Información y Tecnologías COBIT, a fin de identificar debilidades y emitir recomendaciones dentro del ambiente informático, que permitirá eliminar o minimizar los riesgos en los procesos dentro de la Institución.

1.4.2 Objetivos Específicos

- Elaborar el Plan de investigación de campo o programa de auditoría.
- Recopilar información que detalle la situación actual del sistema de información.
- Realizar el análisis de la información recopilada.
- Determinar los niveles de madurez.
- Verificar las observaciones.
- Elaborar el informe borrador.
- Validar el informe borrador.
- Elaborar y entregar el informe final.

1.5 Justificación

El uso de estándares de Tecnologías de Información para la realización de una Auditoría Informática son fundamentales, no solo muestran las necesidades de la Gestión de TI sino que ayudan a encontrar los riesgos del negocio, estableciendo los controles necesarios.

La solución que se ha propuesto es una Auditoría Informática de manera inmediata, para luego con los resultados obtenidos alcanzar un informe que ayude a rectificar errores y que la Institución pueda tomar decisiones de acuerdo a sus necesidades y presupuesto, es decir decisiones acertadas con el fin de mejorar la productividad del Departamento Informático.

Los motivos por los cuales se optó por el estándar COBIT, se deben principalmente a que este incluye las mejores prácticas en tecnología alineadas al gobierno de las tecnologías de información junto a Guías de Auditoría. Esta evaluación permitirá recoger, agrupar y evaluar evidencias para determinar si el sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

Las organizaciones actualmente necesitan mantener un control interno y COBIT tiene el marco organizativo que proporciona un enfoque total hacia las Tecnologías de Información, lo cual representa un valor agregado a sus planes y objetivos dando ventaja competitiva a las empresas.

De esta forma el COMIL Nº 10 ganará eficiencia, eficacia, rentabilidad y seguridad en cada uno de sus procesos. Todo esto se realizará bajo los lineamientos y herramientas estándares de COBIT.

1.6 Alcance

El proyecto de Tesis consiste en una Evaluación Técnica Informática del Sistema de Información del COMIL Nº 10 ABDÓN CALDERÓN, localizado en el sector del Pintado, en la ciudad de Quito. Se utilizará el Estándar Internacional Objetivos de Control para la Información y Tecnologías (COBIT), como un medio de control de la TI, basado en criterios de negocios, documentado por objetivos de control, organizado en dominios, procesos y actividades TI.

Provee 34 objetivos de control agrupados en cuatro dominios:

- Planificación y Organización.
- Adquisición e Implementación.
- Entrega y Soporte.
- Monitoreo y Evaluación.

Se hará uso de una matriz de riesgos, esta herramienta de control y de gestión se utilizará para identificar las actividades (procesos y productos) más importantes del COMIL Nº 10, el nivel de riesgos y vulnerabilidades relacionadas con TI. Igualmente, la matriz de riesgo determinará el grado de protección global y calificará la efectividad de cada control para el riesgo, permitiendo evaluar la efectividad de una adecuada gestión y administración de los riesgos que pudieran impactar los resultados y por ende al logro de los objetivos de la Institución.

La matriz, como una herramienta flexible, documentará los procesos y evaluará de manera integral el riesgo dentro de la Institución, a partir de los

cuales se realiza un diagnóstico objetivo de la situación global de riesgo de la entidad a fin de identificar debilidades para desarrollar un Informe y emitir recomendaciones que permitan mitigar los riesgos del Centro de Informática de la Institución.

1.7 Metodología de Aplicación

A continuación se define la metodología que será utilizada en el proyecto para comprender mejor y poder realizar un estudio objetivo:

La Auditoría en Base a Riesgos (ABR), es una normativa técnica que identifica los riesgos de TI, el cumplimiento de los requisitos técnicos y medios de verificación mediante la Matriz de Riesgos que se usará para determinar los puntos críticos a evaluar, los objetivos específicos de auditoría y los procedimientos o pruebas de auditoría.

Para la Evaluación Técnica Informática del Sistema de Información del COMIL Nº 10 se aplicará el estándar internacional COBIT Objetivos de Control para la Información y Tecnologías (COBIT, en inglés: Control Objectives for Information and related Technology) se origina en el ámbito de la Auditoría de Sistemas y está orientado al control de las actividades y se dirige principalmente a las gerencias, no sólo se focaliza en los servicios de explotación sino que cubre todo el espectro relacionado con los sistemas y tecnologías de la información. [2]

[2] **Tomado de la URL**: *www.helkyncoello.wordpress.com/2008/12/08/itil-cobit-cmmi-pmbok-como-integrar-y-adoptar-los-estandares-para-un-buen-gobierno-de-ti/*

COBIT tiene su base en los objetivos de control de ISACF actualmente conocida como ISACA (Asociación para el Control y Auditoría de Sistemas de la Información), pero han sido mejorados de acuerdo a los actuales estándares internacionales profesionales y específicos a la industria, este modelo de referencia tiene la facilidad de adaptarse a cualquier tipo de negocio y los objetivos de control que se han definido en el modelo pueden ser aplicados independientemente del ambiente, plataformas y madurez tecnológica de la organización, por ello es necesario aplicar este estándar a la Evaluación Técnica Informática.

COBIT, es una herramienta desarrollada para ayudar a los administradores de negocios a entender y administrar los riesgos asociados con la implementación de nuevas tecnologías y demostrar a las entidades reguladoras e inversionistas, que tan efectiva es su tarea.

Se ha definido a COBIT como: "una estructura de relaciones y procesos para direccionar y controlar la compañía para lograr la consecución de los objetivos del negocio, entregando valor agregado mientras se administra el riesgo en función del ambiente de sistemas y sus procesos".

CAPÍTULO 2

FUNDAMENTO TEÓRICO

2.1 Introducción

La importancia que las TI han alcanzado hoy en día es enorme. Ha dejado de ser una herramienta de soporte y/o un área accesoria para convertirse en algo totalmente necesario para cualquier empresa.

La primera generación de computadoras estaba destinada a guardar los registros y monitorear el desempeño operativo de la empresa, pero la información no era oportuna ya que el análisis obtenido en un día determinado en realidad describía lo que había pasado una semana antes. Los avances actuales hacen posible capturar y utilizar la información en el momento que se genera, es decir, tener procesos en línea. Este hecho no sólo ha cambiado la forma de hacer el trabajo y el lugar de trabajo sino que también ha tenido un gran impacto en la forma en la que las empresas compiten (Alter, 1999).

Es impensable concebir una empresa que no use las tecnologías de la información para la gestión del día a día; desde las formas más básicas como el uso de una herramienta ofimática o del correo electrónico hasta implantaciones de inteligencia de negocios y explotación de datos. Pero de cualquier modo, son muchos los problemas que se presentan al gestionar estas Tecnologías de la Información, principalmente en el sentido de cómo lograr que las TI conlleven a una ventaja para la organización, como hacer que las TI sean una inversión con retorno y no solamente un gasto necesario.

Es por ello que se han creado en la industria diversos marcos de trabajo y mejores prácticas que buscan eliminar estas problemáticas. Estas mejores prácticas se han convertido en estándares de la industria, tales es así que su implantación se ha transformado en los últimos años en una necesidad para aquellas empresas que deseen gestionar las TI adecuadamente y lograr ventajas de negocio de las mismas.

2.2 Tecnologías de la Información

La Tecnología de la Información (TI) se entiende como aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información. La tecnología de la información se encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones (Bologna Walsh, 1997).

El desarrollo tecnológico es un proceso complejo, que implica más que la aceptación de los adelantos materiales y técnicos, es un proceso cultural, social y psicológico, al cual corresponden cambios de las actitudes, pensamientos, valores, creencias y comportamientos. La tecnología es la principal herramienta de trabajo del hombre, pero como toda herramienta, para sacarle el máximo provecho, hay que conocerla y utilizarla correctamente, en función de su impacto sociocultural, esto implica la construcción de una cultura tecnológica. Por cultura tecnológica se entiende un amplio espectro que abarca teoría y práctica, conocimientos y habilidades, sumados a una actitud creativa que posibilite a no ser espectadores pasivos en este mundo tecnológico. La cultura tecnológica debe aportar una visión integradora de

todas las modalidades de la conducta humana y una concepción del hombre como una unidad que se compromete con todas sus potencialidades en todos sus actos.

La tecnología de la Información (TI) está cambiando la forma tradicional de hacer las cosas, las personas que trabajan en gobierno, en empresas privadas, que dirigen personal o que trabajan como profesional en cualquier campo utilizan la TI cotidianamente mediante el uso de Internet, las tarjetas de crédito, el pago electrónico de la nómina, entre otras funciones.

El uso creativo de la tecnología de la información puede proporcionar a los administradores una nueva herramienta para diferenciar sus recursos humanos, productos y/o servicios respecto de sus competidores (Alter, 1999).

2.2.1 Tecnologías de Información en la Empresa

Existe una relación bidireccional entre la organización y sus sistemas de información. La organización está abierta a los impactos de los sistemas de información y estos deben estar alineados con los objetivos de la organización. Existen unos factores mediadores que influyen en la interacción entre las Tecnologías de Información y las organizaciones.

Figura 2. 1 Centro de la Tecnología de la Información

Las TIC[3] pueden usarse simplemente para automatizar procesos preexistentes, pero lo más probable es que las actividades sean por lo menos racionalizadas, para aprovechar las ventajas de la nuevas posibilidades que la tecnología crea, y en algunos casos los procesos requieren ser rediseñados sustancialmente. Por lo tanto, los impactos sobre los procesos organizacionales son notorios y pueden ser muy profundos.

No existe la madurez en relación con las empresas que adopten prácticas de gobierno de TI, muchas tecnologías se han incorporado a la organización en respuesta a las necesidades inmediatas y al aumento de la complejidad de los entornos de TI. Junto a ese factor es también la cuestión del crecimiento o la expansión de las empresas, incluida la que conduce ampliar sus instalaciones, no sólo dentro del país sino también en el extranjero.

[3] **TIC** – *Tecnologías de la Información y la Comunicación.*

2.2.2 El Valor de la Información en las Empresas

Al implantar nuevas tecnologías de informática y comunicaciones, los patrones de trabajo y las habilidades que las empresas requieren, podrán ser muy diferentes de los que se tenían antes. Son vitales las capacidades relacionadas con la información y las comunicaciones, estas tecnologías ofrecen la posibilidad de desarrollar trabajos en la sede del cliente, o en la residencia del trabajador, manteniendo en todo momento la necesaria comunicación e intercambio de información con la empresa.

La estructura organizacional se ve impactada por las Tecnologías de Información de manera creciente, el enfoque tiende a dar trascendencia a los procesos del negocio, y a considerar como menos importante la jerarquía de administradores y supervisores. Las unidades organizacionales que funcionan como mini imperios son a menudo ineficientes por su resistencia al cambio. Cuando se implementan tecnologías informáticas y de comunicaciones, esas unidades tienden a ser remplazadas por grupos más sueltos, no asociados por líneas funcionales, como mercadeo o producción, sino a lo largo de la cadena de negocios que añade valor a la materia prima para producir productos finales.

2.3 Introducción a la Auditoría Informática

Las empresas en general, con sus procesos internos son cada vez más dependientes de los recursos de Tecnologías de la Información (TI), lo que implica una creciente necesidad para que la gestión de riesgos en TI no ponga en peligro la continuidad del negocio.

Hace unos años, el mercado de TI tenía una tendencia en buscar la alineación con el negocio. En este contexto, tenía el objetivo táctico y operativo, y fue tratado en general como un centro de costos. Su papel consistía en apoyar la estrategia de negocio y tenía que ser ágil. Sin embargo, el mercado actual muestra que la agilidad y la alineación son importantes pero no suficientes, tiene que ser un medio de activación de la compañía, se convierte en parte de la estrategia empresarial, que funciona de forma totalmente orientada al servicio para que el área de TI funcione aprovechando la ventaja competitiva.

En Estados Unidos por ejemplo para negociar la **Bolsa de valores de Nueva York** (NYSE), las empresas necesitan satisfacer los requisitos de la Ley **Sarbanes-Oxley** (SOX) que consiste en monitorizar a las empresas que cotizan en bolsa de valores, evitando que las acciones de las mismas sean alteradas de manera dudosa. Esto, a su vez, determina la creación de la **Public Company Accounting Oversight Board** (PCAOB), que es la junta de auditores de las sociedades cotizadas.

La misión de la PCAOB es establecer las normas de auditoría, control de calidad, la ética y la independencia en relación con los procesos de inspección y emisión de informes de auditoría. El PCAOB recomienda que las compañías

utilicen un marco apropiado y reconocido en el mercado para evaluar sus controles internos, y menciona específicamente el marco COSO (Committee of Sponsoring Organizations) modelo de control utilizado en la Auditoría Interna.

En cuanto al gobierno de TI, el marco de trabajo de control de COBIT para los procesos de TI que mejor se adapta a los requerimientos de COSO, se encuentra en un nivel más estratégico, y sugiere el uso de otros marcos de trabajo que pueden ser vistos como complementarios y necesarios a fin de establecer un modelo de gobierno de TI.

2.3.1 Conceptos de Auditoría y Auditoría Informática

Auditoría

Inicialmente, la auditoría se limito a las verificaciones de los registros contables, dedicándose a observar si los mismos eran exactos. Por lo tanto esta era la forma primaria: confrontar lo escrito con las pruebas de lo acontecido y las respectivas referencias de los registros; con el tiempo, el campo de acción de la auditoría ha continuado extendiéndose, no obstante son muchos los que todavía la juzgan como portadora exclusiva de aquel objeto remoto, o sea, observar la veracidad y exactitud de los registros.

Con este criterio la Auditoría es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado. El auditor observa la exactitud, integridad y autenticidad de tales demostraciones, registros y documentos. Y consiste en apoyar a los miembros de la empresa en el desempeño de sus actividades. Para ello la Auditoría les

proporciona análisis, evaluaciones, recomendaciones, asesoría e información concerniente a las actividades revisadas.

Objetivos de la Auditoría:

- Mejorar la administración mediante la implantación de recomendaciones;
- Asegurar la ética en la administración, por medio de un eficiente control posterior;
- Verificar la confiabilidad, oportunidad y pertinencia de la información financiera y administrativa;
- Poner de manifiesto y corregir las irregularidades, errores, desviaciones o deficiencias de las operaciones;
- Verificar que los recursos humanos, materiales y financieros hayan sido debidamente controlados y aplicados a los programas, actividades y propósitos autorizados y que hayan sido utilizados de manera eficiente, efectiva y económica;
- Comprobar el cumplimiento de las disposiciones legales referentes a la gestión administrativa y financiera;
- Determinar si todas las rentas e ingresos resultantes de las operaciones han sido correctamente determinados, cobrados y contabilizados;
- Evaluar los sistemas de control interno y formular recomendaciones para mejorarlos.

Auditoría Informática

Es el examen objetivo, crítico, sistemático, posterior y selectivo que se hace a la administración informática de una organización, con el fin de emitir una opinión acerca de la eficiencia en la adquisición y utilización de los recursos informáticos, la confiabilidad, integridad, seguridad y oportunidad de la información y la efectividad de los controles en los sistemas de información.

Es parte de la Auditoría Operacional y consiste en la verificación y evaluación de los procedimientos de informática, sistemas y equipos de cómputo, a fin de lograr una utilización más eficiente y segura, que servirá para una adecuada toma de decisiones.

La auditoría informática debe ser:

- Objetiva, porque requiere un alto grado de independencia mental del auditor, con relación a los funcionarios y actividades de las entidades auditadas.
- Crítica, porque el auditor requiere de evidencias para poder emitir una opinión sobre los procesos auditados.
- Sistemática, por cuanto se basa en normas, métodos, procedimientos y técnicas de auditoría de sistemas.
- Posterior a las actividades, operaciones y decisiones tomadas por la entidad vigilada.
- Selectiva a través de muestras. El auditor debe determinar el tamaño de la muestra para poder, si es del caso, inferir conclusiones generales.

2.3.2 Tipos de Auditoría Informática

2.3.2.1 Auditoría Interna

Consiste en el examen y evaluación de las transacciones y operaciones financieras y administrativas de una entidad u organismo, como un servicio a la alta dirección, realizada por auditores organizados en una unidad administrativa de auditoría interna; las funciones de estos auditores deben estar completamente desligadas de las actividades sujetas a su examen. Las auditorías internas, además de sus funciones específicas, proporcionan la asesoría técnica administrativa que les sea solicitada.

La unidad de auditoría interna debe tener el máximo grado de independencia. La función del personal de auditoría es la evaluación y juzgamiento y no participa en los procesos de administración, aprobación, contabilización o adopción de decisiones dentro de la entidad y organismo. Su participación en las actividades de toma de inventarios físicos, entrega recepciones, avalúos, remates, bajas y otros actos similares, se limitará a observar dichas actividades, sin aprobar ni firmar los documentos respectivos, debiendo informar separadamente.

2.3.2.2 Auditoría Externa

Es el examen crítico, sistemático y detallado de un sistema de información de una unidad económica, realizado por un Contador Público sin vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir una opinión independiente sobre la forma como opera el sistema, el control interno del mismo y formular sugerencias para su

mejoramiento. El dictamen u opinión independiente tiene trascendencia a los terceros, pues da plena validez a la información generada por el sistema ya que se produce bajo la figura de la Fe Pública, que obliga a los mismos a tener plena credibilidad en la información examinada.

La Auditoría Externa examina y evalúa cualquiera de los sistemas de información de una organización y emite una opinión independiente sobre los mismos, pero las empresas generalmente requieren de la evaluación de su sistema de información financiero en forma independiente para otorgarle validez ante los usuarios del producto de este, por lo cual tradicionalmente se ha asociado el término Auditoría Externa a Auditoría de Estados Financieros, lo cual como se observa no es totalmente equivalente, pues puede existir Auditoría Externa del Sistema de Información Tributario, Auditoría Externa del Sistema de Información Administrativo, Auditoría Externa del Sistema de Información Automático etc. Y tiene por objeto averiguar la razonabilidad, integridad y autenticidad de los estados, expedientes y documentos y toda aquella información producida por los sistemas de la organización.

Una Auditoría Externa se lleva a cabo cuando se tiene la intención de publicar el producto del sistema de información examinado con el fin de acompañar al mismo una opinión independiente que le dé autenticidad y permita a los usuarios de dicha información tomar decisiones confiando en las declaraciones del Auditor.

2.3.3 Modelos de Control Utilizados en la Auditoría

"**COBIT**, (Control Objectives for Information and related Technology), es un marco de referencia de gobierno de TI que relaciona procesos, recursos e información con los objetivos de negocio de una organización para gestión y control de las Tecnologías de la Información. Consiste en un conjunto de documentos que define un marco de trabajo para permitir que las organizaciones alcancen sus objetivos. [4] "

"**ITIL** (Information Technology and Infraestructure Library) es un estándar para la gestión de los servicios de Tecnologías de la Información (TI). Su objetivo principal es aportar un enfoque orientado al proceso para la entrega de la infraestructura TI como un conjunto de servicios y el soporte directo de esos servicios. Se centra en brindar servicios de alta calidad determinando la forma de ejecutar procesos estándar ayudados de la tecnología para lograr la satisfacción de las personas, usuarios de los servicios de TI. [5] "

"**COSO** La actual definición del control interno emitida por The Committee of Sponsoring Organizations of the Treadway Commission de los Estados Unidos de Norteamérica, a través del documento denominado "Control Interno-Marco Integrado" mejor conocido como el Modelo de Control COSO, amplia el concepto de la siguiente manera: un proceso efectuado por la Junta Directiva de la entidad, por la Administración y por otro personal diseñado para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. [6] "

[4] **Tomado de la URL:** *www.redindustria.blogspot.com/2009/01/cobit-itil.html*
[5] **Tomado de la URL:** *www.redindustria.blogspot.com/2009/01/cobit-itil.html*
[6] **Tomado de la URL:** *www.cemla.org/old/pdf/aud-991109-mex.PDF*

"La norma **ISO/IEC 17799** (denominada también como **ISO 27002**) es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000, con el título de Information technology - Security techniques - Code of practice for information security management. Tras un período de revisión y actualización de los contenidos del estándar se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. El estándar ISO/IEC 17799 tiene su origen en Archivo:La norma británica British Standard BS 7799-1 que fue publicada por primera vez en 1995. [7] "

"La norma **ISO/IEC 27001** (Information technology - Security techniques - Information security management systems - Requirements) fue aprobada y publicada como estándar internacional en Octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming". Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la revisión de la norma británica British Standard BS 7799-2:2002. [8] "

[7] **Tomado de la URL:** *www.itnews.ec/marco/000130.aspx*
[8] **Tomado de la URL:** *www.eserna.com/Interes/indexn.html*

Tabla 2. 1 Tabla Comparativa de Metodologías

	COBIT	ITIL	COSO	ISO 27001
AUTORES	Organizaciones de Tecnologías de Información como ISACA	Brian Johnson, quien formó parte del equipo del gobierno británico que creó ITIL y proveedores de servicios de Tecnologías de Información	Organizaciones de Tecnologías de Información COSO	Proveedores de cualquier tipo de producto / servicio
ALCANCE	Auditoría y control de Sistemas de Información. Alineamiento y gobierno de Tecnologías de Información	Tiene un enfoque sistemático del servicio TI centrado en los procesos y procedimientos junto al establecimiento de estrategias para la gestión operativa de la infraestructura TI	Proporciona un control interno a la administración con un aseguramiento razonable con respecto al logro de los objetivos	Requerimientos para establecer un sistema de gestión de seguridad de la información dentro del contexto de riesgos generales de la organización
TAMAÑO	Provee 34 procesos de TI, 210 objetivos de control agrupados en cuatro dominios	Dos libros centrales, que cubren las áreas de Soporte del Servicio y Prestación del Servicio	El modelo identifica 3 Objetivos de control interno y 5 componentes que contienen 17 factores	Existen 39 categorías y varios controles han sido añadidos para llegar a un total de 133

	COBIT	ITIL	COSO	ISO 27001
DOCUMENTOS RESULTANTES	Certificación de ISACA para ser CISA Certified Information Systems Auditor. Reporte del Auditor; no hay certificación formal para la empresa.	La fundación holandesa "Exameninstituut voor Informatica" (EXIN) y la inglesa "Information Systems Examination Board" (ISEB) en estrecha cooperación con la OGC y el itSMF ofrecen certificaciones en tres niveles: • Foundation Certificate en Gestión de Servicios TI. • Practitioner Certificate en Gestión de Servicios TI. • Manager Certificate en Gestión de Servicios TI	Reporte de evaluación; no hay certificación formal	Certificación por entes autorizados.
ORIENTACIÓN	Gobierno Control y Auditoría	Soporte del servicio y Prestación del servicio	Mejores prácticas en la Auditoría Interna	Sistemas de Gestión de Seguridad de la Información

Las características de COBIT coloca en un nivel más estratégico, en comparación con otros frameworks, las normas que complementan la Figura 2.2 Ilustra la posición y los puntos de integración de COBIT con respecto a otros modelos.

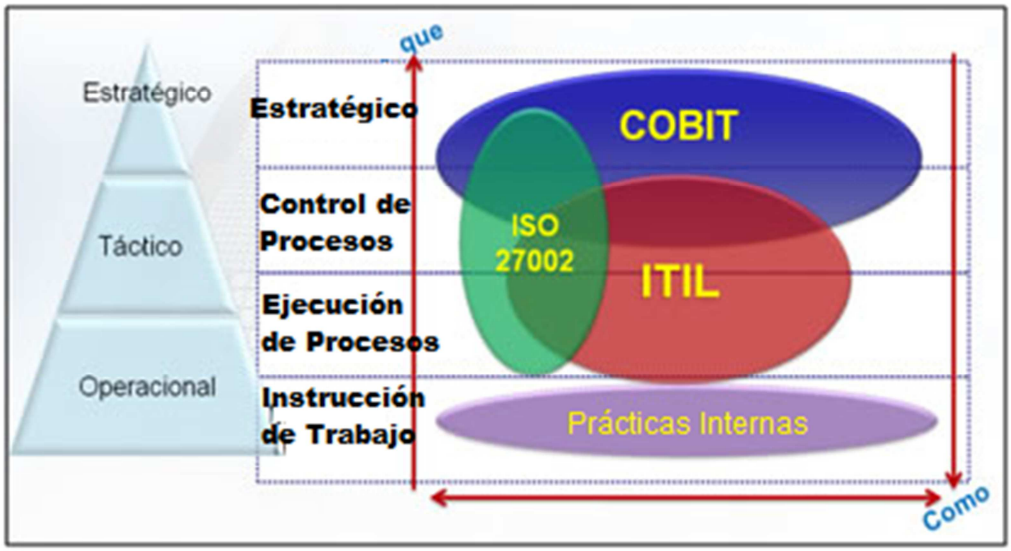


Figura 2. 2 Modelos, referencia y guías de mejores prácticas puede ser usado para establecer un modelo de gestión para las organizaciones de TI.

Los ejecutivos pueden evaluar cuál es el mejor modelo para satisfacer las necesidades comerciales de sus empresas, pero está claro que la regulación externa dirige con fuerza la adopción de COBIT en sus prácticas de gobierno de TI. Un factor muy importante es que el framework de COBIT como un control de alto nivel, señala lo que debe ser controlado pero no dice cómo. Se adapta perfectamente a las mejores prácticas para la gestión de los servicios de TI que se describen en la IT Infrastructure Library (ITIL), se centra más procedimientos tácticos y operativos en relación con los internos de TI.

2.3.4 Principios de COBIT

Es el fundamento para las buenas prácticas de seguridad, porque proporciona directrices sobre la adopción de un estándar de gobierno y control de TI, cubre la seguridad y otros riesgos que se producen en los ambientes de TI.

La seguridad no es un esfuerzo de una sola vez, se debe administrar el esfuerzo aplicado a proteger el ambiente de trabajo sobre la base de las consecuencias de un impacto de un problema de seguridad, donde la buena seguridad mejorará la reputación, la confidencialidad y la confianza de otros con quienes se dirige el negocio, ahorrando tiempo y dinero.

A continuación se presenta la figura 2.3 que sintetiza los principios de COBIT.

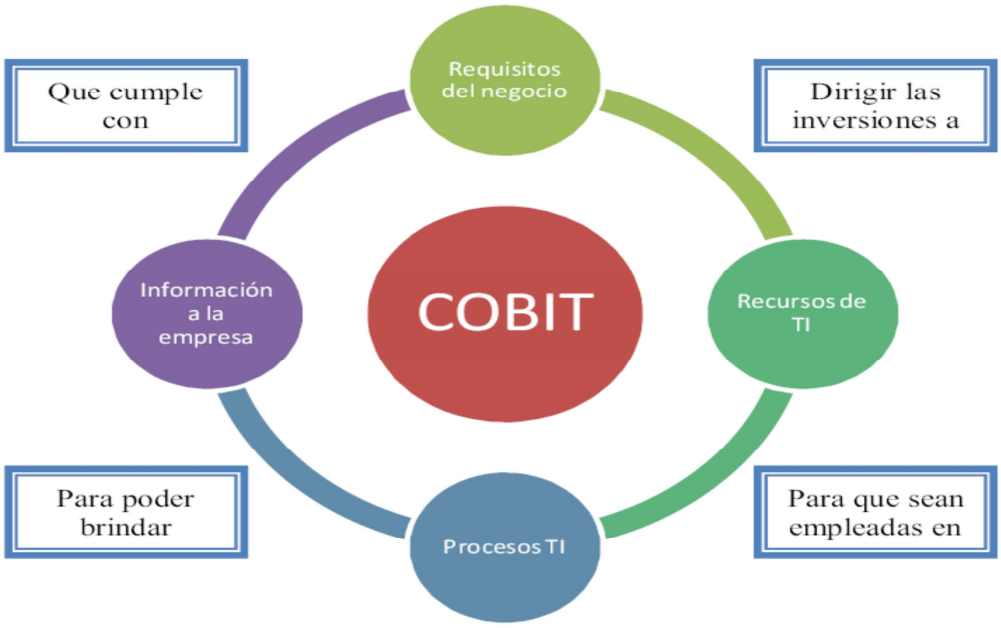


Figura 2. 3 Principios de COBIT

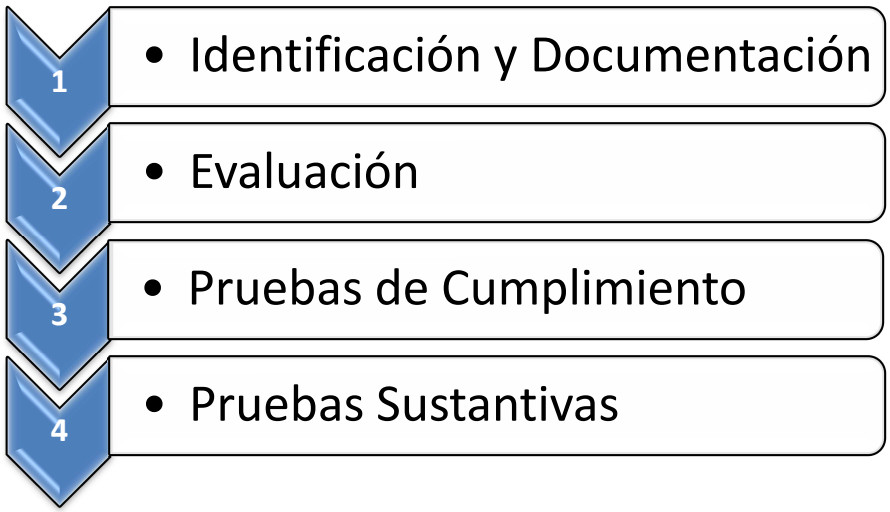
2.3.5 Estructura del Proceso de la Auditoría Informática

Definir el alcance de la auditoría es crucial para el dimensionamiento como el esfuerzo necesario para llevar a cabo este proceso de control. Para que esto se haga correctamente, es importante tener en cuenta la preocupación por los procesos de negocio, plataformas, sistemas y su relación, finalmente con las funciones y responsabilidades en la estructura organizativa.

El siguiente paso es identificar los requerimientos de información relacionados con los procesos de negocio. Para ello es esencial entender cuál es la relevancia de cada proceso. Además es necesario identificar los riesgos inherentes a los procesos de TI y un nivel de control global.

Se debe seleccionar cuáles son los procesos y plataformas que van a ser auditados. Esto ayuda a centrarse en los temas más relevantes, creando una estrategia de auditoría, aquí es donde se evalúa cuáles son los controles disponibles para los riesgos identificados, cuáles son los pasos y las tareas necesarias para llevar a cabo la auditoría y cuáles son los puntos de decisión.

Generalmente la estructura del proceso de auditoría, aceptado normalmente por el mercado comprende cuatro pasos o etapas principales, como se muestra en el Cuadro 2.1.



Cuadro 2. 1 Estructura del Proceso de la Auditoría

Un proceso de TI es auditado por la comprensión de los riesgos asociados con los requerimientos del negocio y con las medidas de control pertinentes para cada riesgo identificado.

Desde este escenario, se realiza la evaluación del cumplimiento con las pruebas que permitan verificar si un punto de control en particular está funcionando según lo previsto.

Por último, se ejecuta la sustanciación de riesgos relacionados a los objetivos de control que no son alcanzados. Esto puede hacerse mediante técnicas de análisis o utilizando referencias alternativas.

2.3.6 Fases de la Auditoría Informática

FASE I: Conocimientos del Sistema

Aspectos Legales y Políticas Internas. Sobre estos elementos está construido el sistema de control y por lo tanto constituyen el marco de referencia para su evaluación.

Características del Sistema

- Organigrama del área que participa en el sistema
- Manual de funciones de las personas que participan en los procesos del sistema
- Informes de auditoría realizadas anteriormente

Características de la Aplicación

- Manual técnico de la aplicación del sistema
- Funcionarios (usuarios) autorizados para administrar la aplicación
- Equipos utilizados en la aplicación de computadora
- Seguridad de la aplicación (claves de acceso)
- Procedimientos para generación y almacenamiento de los archivos de la aplicación.

FASE II: Análisis de riesgos y amenazas

Identificación de Riesgos

- Daños físicos o destrucción de los recursos
- Pérdida por fraude o desfalco
- Extravío de documentos fuente, archivos o informes

- Robo de dispositivos o medios de almacenamiento
- Interrupción de las operaciones del negocio
- Pérdida de integridad de los datos
- Ineficiencia de operaciones
- Errores

Identificación de las Amenazas

- Amenazas sobre los equipos
- Amenazas sobre documentos fuente
- Amenazas sobre programas de aplicaciones

Relación entre recursos, amenazas y riesgos: La relación entre estos elementos deberá establecerse a partir de la observación de los recursos en su ambiente real de funcionamiento.

FASE III: Análisis de controles

Codificación de controles: Los controles se aplican a los diferentes grupos utilizadores de recursos, luego la identificación de los controles deben contener una codificación la cual identifique el grupo al cual pertenece el recurso protegido.

Análisis de cobertura de los controles requeridos: Este análisis tiene como propósito determinar si los controles que el auditor identificó como necesarios proveen una protección adecuada de los recursos.

FASE IV: Evaluación de Controles

Objetivos de la evaluación

- *Verificar la existencia de los controles requeridos*
- *Determinar la operatividad y suficiencia de los controles existentes*

Plan de pruebas de los controles

- Incluye la selección del tipo de prueba a realizar.
- Debe solicitarse al área respectiva, todos los elementos necesarios de prueba.

Pruebas de controles

FASE V: Informe de Auditoría

Informe detallado de recomendaciones

Evaluación de las respuestas

Informe resumen para la alta gerencia: Este informe debe prepararse una vez obtenidas y analizadas las respuestas de compromiso de las áreas.

- Opinión: con relación a la suficiencia del control interno del sistema evaluado
- Hallazgos
- Recomendaciones

FASE VI: Seguimiento de Recomendaciones

Informes del seguimiento: Evaluación de los controles implantados

2.4 Análisis del Estándar COBIT

2.4.1 Introducción a COBIT

COBIT (Control Objectives for Information and related Technology) permite aplicar las mejores prácticas de marketing para la gestión de riesgos de TI y a través de esta iniciativa, no sólo alcanzar la excelencia operacional, sino también para establecer un modelo de gobierno que mantiene el área de TI integrados con los objetivos empresariales y ofrecer las condiciones apropiadas para la compañía a alcanzar sus objetivos estratégicos.

El marco de trabajo de COBIT tiene un triple enfoque:

Enfocado al management: Puesto que provee a la Administración de una base de mejores prácticas con las cuales se pueden tomar decisiones de TI e inversión.

Enfocado a los usuarios de IT: Debido a la seguridad que les brinda para el control de objetivos y procesos.

Enfocado a auditores: Debido a que permite identificar problemas de control de TI dentro de la infraestructura de TI de la compañía.

La adopción de COBIT no tiene por objeto controlar todos los procesos, sólo identifica los procesos de TI que están siendo afectados por los riesgos del negocio con el fin de dar prioridad a la gestión de estos procesos. COBIT es independiente de la plataforma adoptada en las empresas de TI, también es totalmente independiente del tipo de negocio y el valor y la cuota de tecnología de la información que tiene en la cadena de producción. Además es

un marco de trabajo de control que indica lo que debe hacerse, pero no dice como se debe hacer.

2.4.2 Descripción de los Dominios de COBIT

El *framework* de COBIT sigue la premisa de que no se puede gestionar lo que no se mide, así propone una serie de objetivos de control y sus indicadores de desempeño en consecuencia, la adopción de medidas de manejo para mitigar riesgos y lograr los resultados deseados.

El *framework* COBIT provee los procesos de TI agrupados en cuatro dominios de la siguiente manera:

1. Planear y Organizar (PO)

El dominio de planificación y organización comprende las tácticas adoptadas por la organización de TI, y se refiere a la identificación de la forma en que pueden contribuir de la mejor manera los objetivos de negocio.

La visión estratégica de las TI debe ser planeada, comunicada y administrada desde diferentes perspectivas. Además, esta área abarca también la organización de TI y la infraestructura de la tecnología que debe implementarse en la organización.

El dominio de la planificación y la organización facilita responder a las preguntas que figuran a continuación:

¿Las estrategias de TI y de negocio están alineadas correctamente?

¿La organización está recibiendo el mejor uso posible de sus recursos?

¿Todos en la organización comprenden los objetivos de TI?

¿Los riesgos son comprendidos y administrados?

¿La calidad de los sistemas de TI son adecuados para las necesidades de la empresa?

2. Adquirir e Implementar (AI)

Para que la estrategia de TI se convierta en una realidad, las soluciones tecnológicas deben ser identificadas, desarrolladas o adquiridas, y como resultado, éstas deben ser aplicadas e integradas en los procesos de negocio.

Así, los cambios y el mantenimiento de los sistemas ya existentes son manejados por este dominio para garantizar que las soluciones continúen atendiendo los objetivos del negocio.

Por lo tanto, el dominio de la adquisición e implementación responden a las siguientes preguntas:

¿Los nuevos proyectos que estén en camino ofrecen soluciones que satisfagan las necesidades del negocio?

¿Los nuevos proyectos se llevan a cabo de manera que las entregas se realizan dentro del tiempo asignado y dentro del presupuesto establecido?

¿Los nuevos sistemas funcionarán correctamente cuando se implementen?

¿Los cambios en la infraestructura se realizarán sin causar impactos negativos en el funcionamiento de la empresa?

3. Entrega y Soporte (DS)

Este dominio se centra en la prestación efectiva de los servicios requeridos, y esto incluye la prestación de servicios, gestión de la seguridad y la continuidad de los servicios de TI, servicios de soporte, gestión de datos y el funcionamiento de las instalaciones.

Es evidente para aquellos que han estudiado ITIL encontrar similitud en los objetivos de control ya que COBIT aborda este dominio con las disciplinas de ITIL, sin embargo COBIT se centra más en el control y señala lo que debe ser controlado, en ningún momento el framework COBIT establece cómo deben ser implementados.

Las prácticas descritas en ITIL ofrecen más detalles para que se estructuren los procesos que son ejecutados, por lo que ITIL y COBIT pueden ser integrados sin problemas.

El dominio de entrega y soporte demanda que las administraciones respondan las siguientes preguntas:

¿Los servicios de TI son otorgados organizadamente con las prioridades del negocio?

¿Los costos de TI se han optimizado?

¿La fuerza de trabajo es capaz de utilizar los sistemas de manera productiva y segura?

¿Hay niveles apropiados de confidencialidad, integridad y disponibilidad de seguridad de la información?

4. Monitorear y Evaluar (ME)

El dominio del monitoreo y evaluación considera que todos los procesos de TI deben ser evaluados regularmente en el tiempo, considerando su calidad apegado a los requisitos de control.

Este es el dominio que incluye la gestión del rendimiento, la supervisión de los controles internos, el cumplimiento de leyes y reglamentos específicos, y el gobierno propiamente dicho.

Los procesos de este dominio son tratados con el fin de responder a las siguientes preguntas de gestión:

¿El rendimiento de las TI se miden con el fin de identificar los problemas a tiempo antes de que sea tarde?

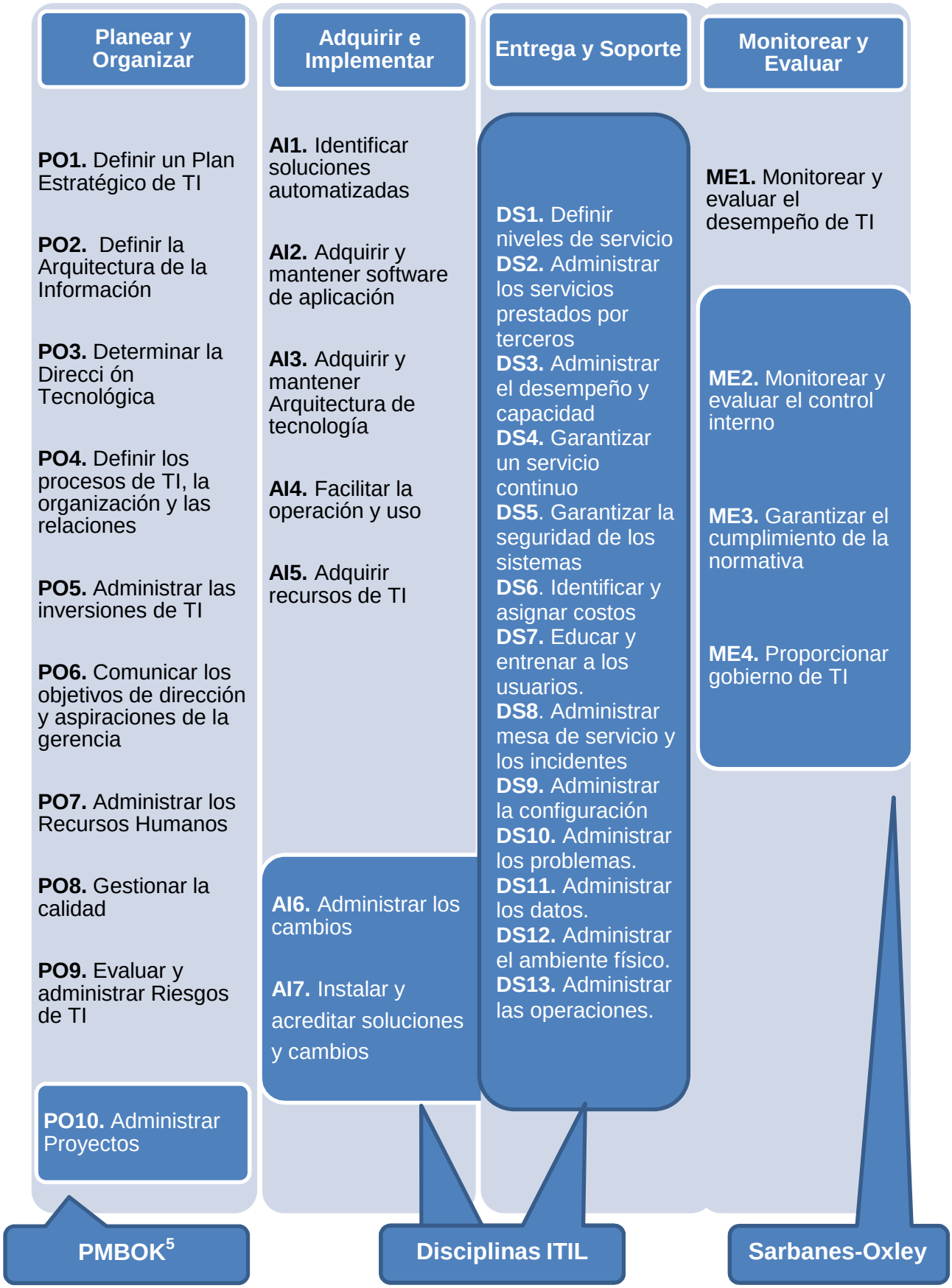
¿La gestión garantiza los controles internos sean efectivos y eficientes?

¿Hay alguna manera de que el rendimiento de las TI estén relacionados con los objetivos de negocio?

¿Hay niveles apropiados de confidencialidad, integridad y disponibilidad en la seguridad de la información?

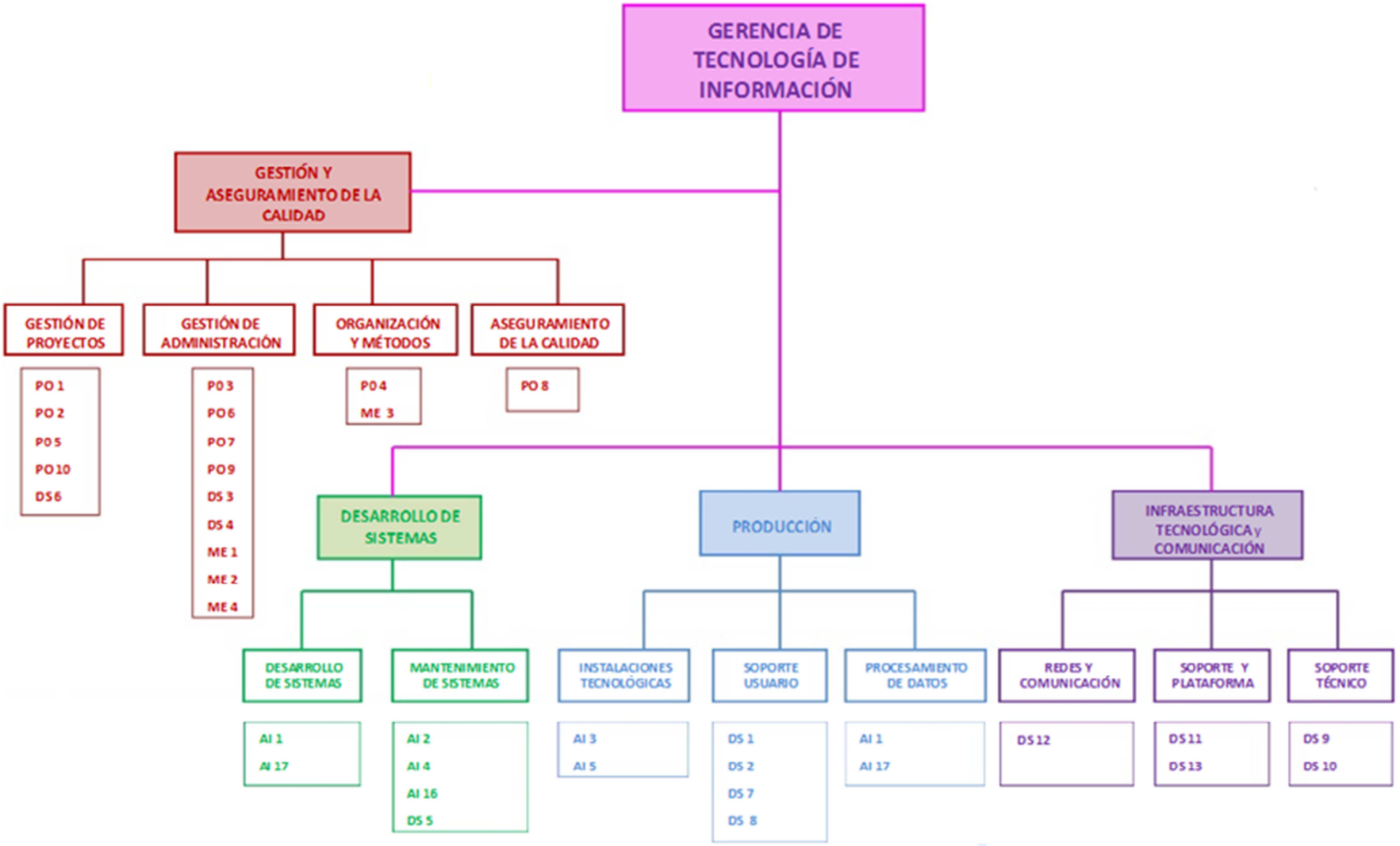
Los siguientes cuadros muestran los 34 Objetivos de Control de alto nivel de COBIT, sus puntos de interacción con otros elementos y su relación con la Gerencia de TI.

Cuadro 2. 2 Dominios y Proceso de COBIT 4.1



[9] **PMBOK** - *Project Management Body of Knowledge: Estándar en la Administración de proyectos.*

Cuadro 2. 3 Los 34 Objetivos de Control relacionados con la Gerencia de TI



2.4.3 Antecedentes Empresariales Aplicando el Estándar COBIT

Una ventaja importante de COBIT es que proporciona una lista completa de los procesos que se pueden utilizar para evaluar, controlar y supervisar las actividades y responsabilidades, sin embargo no todos ellos deben ser aplicados estrictamente. Alternativamente, los procesos se pueden combinar según las necesidades de la empresa.

A continuación se señalan algunas empresas que han aplicado el *framework COBIT:*

“Se realizó una evaluación del riesgo tecnológico para las Instituciones financieras controladas por la Superintendencia de Bancos y Seguros del Ecuador. Las etapas y actividades planteadas para la metodología de evaluación del riesgo tecnológico, permitieron alcanzar los objetivos propuestos al inicio del proyecto obteniendo un valor cuantificable del grado de cumplimiento en cada uno de los aspectos asociados a la tecnología de información requeridos para la administración del riesgo operativo.

Se estableció los objetivos de control de COBIT satisfaciendo los requerimientos normativos de TI. Reflejado en el mapa de riesgo tecnológico las mediciones de madurez e importancia de los procesos de tecnología de información y se validó la consistencia y efectividad de la metodología por medio de la implementación de un plan piloto en una Institución financiera controlada por la Superintendencia de Bancos y Seguros. La determinación del grado de madurez actual y objetivo para cada proceso de TI permitió obtener resultados más ajustados respecto de la situación real de una Institución financiera.

Se señalan que desde el punto de vista de ITIL, una de las buenas prácticas de tecnología de información, la presente metodología incorpora el modelo de mejora continua del servicio, que establece la visión (cumplimiento normativo), la evaluación de la situación actual (etapa B y nivel de madurez actual), el planteamiento de objetivos (nivel de madurez objetivo), el método para alcanzar los objetivos (recomendaciones), y las mediciones y métricas para evaluar la consecución (mapa de riesgo tecnológico). [10] "

"Se desarrolló una Auditoría Informática, en la Unidad Ejecutora Operación de Rescate Infantil ORI, basada en el marco de referencia COBIT y sus cuatro áreas de trabajo. Para poner en marcha la auditoría fue necesario realizar: entrevistas, aplicación de encuestas, inspecciones y recopilación de la información propia del ORI, con el fin de elaborar diferentes informes, los mismos que sirvieron a los Directivos para la toma de decisiones, y sus propuestas de mejora.

El producto final de esta auditoría fueron dos informes finales, un ejecutivo y un detallado, el primero fue entregado al Director del Departamento de Informática con una visión global de los principales eventos encontrados en la Institución, mientras que el informe detallado identificó claramente cada uno de los objetivos de COBIT con sus respectivas observaciones, causas, efectos y recomendaciones, este informe fue entregado tanto al Director de Informática como al Director Ejecutivo, para que se te tomen las decisiones más acertadas. Las principales propuestas de mejora recomendadas por esta

[10] **Tomado de la TESIS:** *METODOLOGÍA DE EVALUACIÓN DEL RIESGO TECNOLÓGICO EN LAS INSTITUCIONES DEL SISTEMA FINANCIERO ECUATORIANO UTILIZANDO COBIT; Por: Katalina del Rocio Coronel Hoyos (2008) ESPE.*

tesis se basaron en la implementación de un plan estratégico acorde a las metas reales de la organización, un plan de mejoramiento empezando por el soporte al usuario mediante la creación de una mesa de servicio y reestructurar la ubicación física del Departamento de Informática para poseer una verdadera seguridad física y lógica. [11] "

"En la Empresa Minga S.A se realizó una Auditoría de Sistemas Informática utilizando COBIT Objetivos de Control para tecnología de la información al Departamento de Tecnología, se ha elaborado un examen crítico evaluando la eficiencia y eficacia de los procesos informáticos los cuales contienen las observaciones tanto de los auditores como del jefe de tecnología, para mejorar la situación de la empresa; se presentó el informe referencial de prevención contra el delito informático que tiene algunas sugerencias de seguridad de manera genérica que se deberían llevar a cabo en cualquier empresa.

Concluyendo así que el Departamento de TI cumple los objetivos planteados con eficacia, pero no existe forma de medir cuantitativamente ni cualitativamente la eficiencia de cada proceso, causando que tanto el personal técnico, como los usuarios y los mandos gerenciales no conozcan el verdadero impacto, que le representa a la empresa, la inversión realizada en tecnologías de la información, mencionan que las guías de auditoría de COBIT son demasiado extensas para ser aplicadas en las PYMES de Ecuador. Cada

[11] **Tomado de la TESIS:** *AUDITORÍA INFORMÁTICA DE LA UNIDAD EJECUTORA OPERACIÓN RESCATE INFANTIL (ORI) Y SUS 21 COORDINACIONES PROVINCIALES APLICANDO EL ESTÁNDAR COBIT; Por: Gordillo Gutiérrez Andrea De Los Ángeles, Zurita Lozada Mónica Jimena (2008) ESPE*.

empresa es única en sí misma y por lo tanto el Departamento de TI debe acoplarse y buscar las soluciones más viables que cumplan con la seguridad, confiabilidad e integridad, el tener solo una persona que se encargue del desarrollo de software, administración BD y Soporte a usuarios hace que los servicios que brinda el Departamento de TI a la empresa sean postergados y que no exista una planificación adecuada con la cual se pueda verificar que se cubren las necesidades informáticas de la empresa. [12] "

[12] **Tomado de la TESIS:** *AUDITORÍA DE SISTEMAS INFORMÁTICOS EN LA EMPRESA MINGA S.A. Y SU SUCURSAL UTILIZANDO COBIT; Por: Castellano Diana Alejandra, Yonfá Guerrero Bengy Xavier (2009) EPN.*

CAPÍTULO 3

APLICACIÓN DE LA AUDITORÍA INFORMÁTICA UTILIZANDO EL ESTÁNDAR COBIT EN EL COLEGIO MILITAR No.10 “ABDÓN CALDERÓN”

3.1 Recopilación de Información

3.1.1 Compilación de las Actividades del COMIL Nº 10

El Colegio Militar Nº 10 “Abdón Calderón” nació como Casa Maternal el 28 de Noviembre de 1.953, En 1.961, la Dirección Provincial de Educación de Pichincha autorizó el funcionamiento de la Escuela del Ejército “Abdón Calderón”. En 1.996, por disposición de la Dirección de Educación de la Fuerza Terrestre, se fusionan el Jardín de Infantes, la Escuela y Colegio en la Unidad Educativa del Ejército “Abdón Calderón”. En 1.984 se autoriza la creación del Colegio del Ejército. Desde 1999 se crea el Colegio Militar N°10 “ABDÓN CALDERÓN”.

Actualmente es una Institución pública y su Misión es impartir una educación integral a la niñez y juventud en los niveles inicial, básico y bachillerato técnico que contribuya al desarrollo de la sociedad ecuatoriana, a través de un Modelo Pedagógico por competencias, dentro de un marco de lealtad a la Institución, disciplina consciente y práctica permanente de valores.

Tienen como Visión ser una Institución educativa humanista, técnica y con una formación integral, mediante la ejecución de un sistema educativo moderno, eficiente y eficaz, con reconocimiento nacional e internacional,

teniendo como fundamento la Identidad Nacional, el fortalecimiento de valores, la investigación, el fortalecimiento del idioma inglés, el trabajar bajo un sistema de gestión de calidad educativa, utilizando un currículo con enfoque de competencias que relaciona el mundo laboral con el educativo para lograr bachilleres técnicos con especialización en función de las necesidades de desarrollo del país. [13]

3.1.2 Compilación de las Actividades de la Dirección de Tecnologías de Información dentro de la Institución

El COMIL No.10 "ABDÓN CALDERÓN", cuenta a nivel de Dirección de Tecnología de Información con el Departamento Informático denominado “Centro de Informática”. La misión del Centro de Informática es proveer y administrar, los servicios que satisfagan las necesidades informáticas, con el propósito de apoyar a los usuarios de manera eficiente en sus funciones y en los procesos administrativos de la organización.

La Institución dispone a nivel de su estructura tecnológica de un total de 230 computadoras y 45 impresoras, para abastecer las necesidades académicas de 2503 cadetes y administrativas de 240 empleados militares y civiles del plantel. Para brindar soporte técnico a esta cantidad de computadoras y a los usuarios de las mismas el Centro de Informática de la Institución tiene tres personas a su cargo. Además del recurso computacional mencionado anteriormente cuenta con una red administrativa con 48 puntos

[13] **Tomado de la URL:** *www.comil10ac.edu.ec/*

de red en el bachillerato y 10 puntos de red en EGB[14], y una red académica con 88 puntos de red en bachillerato y 19 puntos de red en EGB.

En la parte de software la Institución cuenta a la fecha con 6 sistemas y programas, los mismos que son utilizados por el personal administrativo del COMIL Nº 10, para efectuar los trabajos de las diferentes dependencias: El Sistema Integrado Educativo: académico, de secretaría y de colecturía. El Portal web de la Institución. El Sistema integrado de gestión documental del Estado. El Sistema de Contratación Pública.

3.1.2.1 Funciones del Centro de Informática

Dentro de las funciones que realiza el Centro de Informática del COMIL No.10 "ABDÓN CALDERÓN" son las siguientes:

- Programar y desarrollar los sistemas, las bases de datos adquiridas por la Unidad Educativa.
- Realizar el estudio e investigación de aplicación y combinación de medios múltiples asociados con computación, de acuerdo a las necesidades.
- Realizar el estudio sobre nuevos programas y dar orientación al personal técnico sobre los mismos.
- Asistir técnicamente sobre instalaciones, actualización, funcionamiento y mantenimiento de hardware y software.
- Llevar un registro de todos los programas implementados en el establecimiento educativo.

[14] **EGB** – *Educación General Básica, COMIL-10.*

- Asesorar a los usuarios de la Institución sobre la correcta utilización de la información procesada.
- Operar la Unidad Central de Proceso y velar por el funcionamiento de las redes de comunicación y terminales distribuidos en el establecimiento.
- Administrar el sistema físico y realizar el plan de mantenimiento de los equipos, coordinando con empresas especializadas.
- Mantener actualizados los sistemas de respaldo de la información.
- Preparar y difundir normas y procedimientos que deban utilizarse en el manejo de los equipos.
- Determinar las normas de seguridad de los sistemas.
- Coordinar las actividades de capacitación profesional del personal del Centro de Informática.
- Establecer controles de entrada y salida de información.

3.1.3 Organigrama Funcional del Colegio Militar No.10 “Abdón Calderón”

En la Figura 3.1 se observa el organigrama funcional de la Institución, en la cual se puede identificar los niveles de Dirección como son: Rectorado, Vicerrectorado, Centro de Informática, Departamentos: Académico, Investigación y Evaluación Educativa, Administrativo y Finanzas.

Todos estos organismos constan de una estructura interna que apoya los objetivos encargados a cada una de las Direcciones.

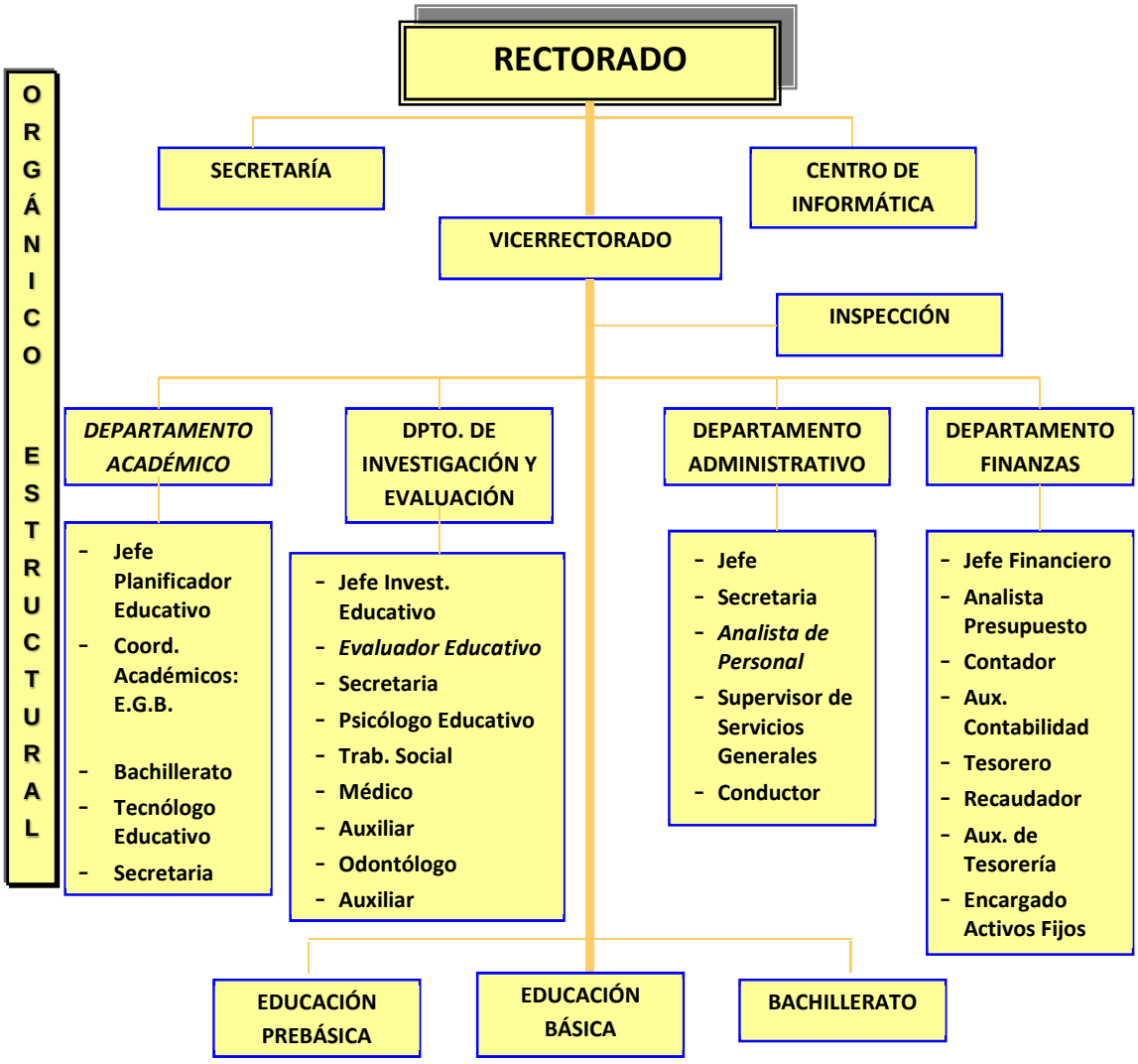


Figura 3. 1 Organigrama funcional de la Institución COMIL Nº 10

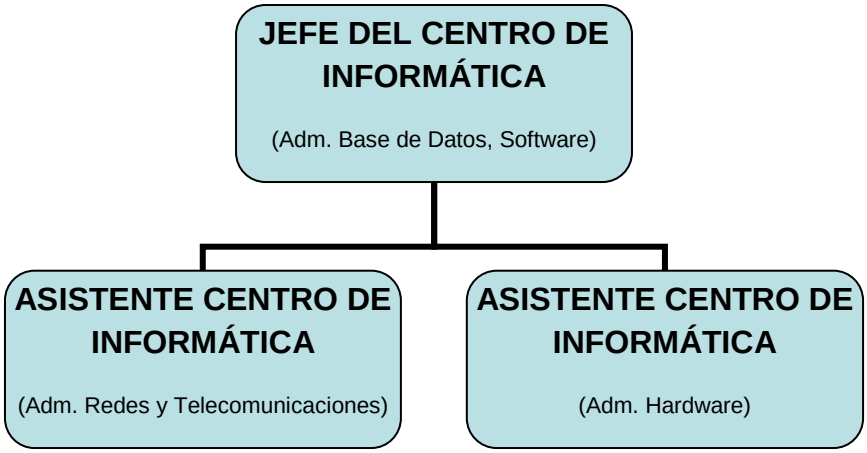
Los niveles de Dirección están liderados por la Dirección Ejecutiva que es el Rectorado y que brinda el respaldo necesario a todas las Direcciones Departamentales. Este apoyo se fundamenta en un proceso que cumple políticas militares a las que permiten fortalecer las áreas principales de la Institución.

El Departamento Informático de la Institución denominado Centro de Informática reporta directamente al Rectorado a nivel de Dirección, éste nivel jerárquico en que se encuentra dentro del organigrama, permite observar que

el servicio apoya además del Rectorado a los Departamentos: Académico, Investigación y Evaluación Educativa, Administrativo y Finanzas.

3.1.4 Estructura Interna del Departamento Informático

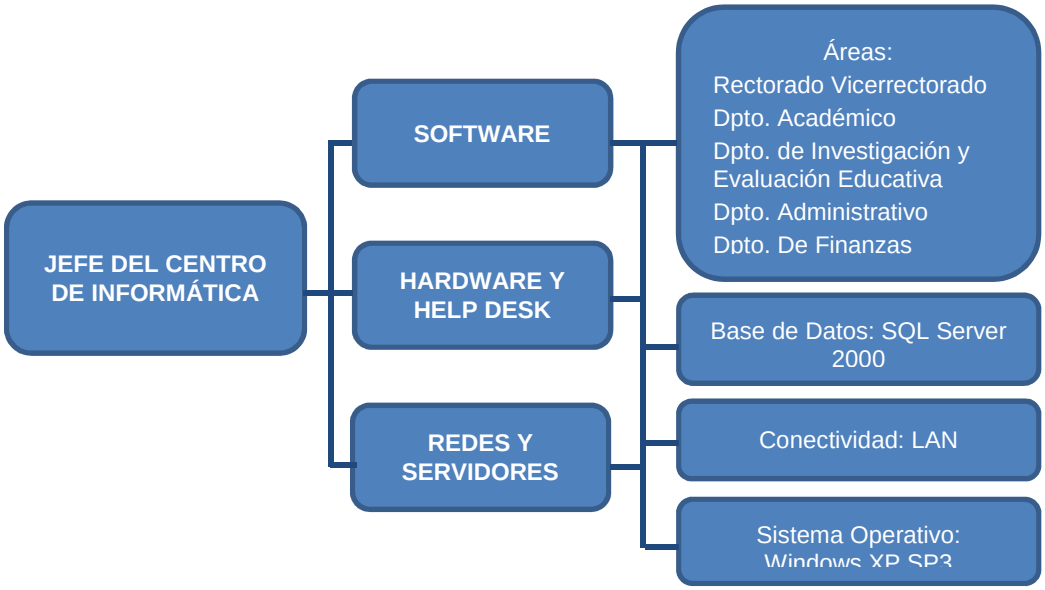
En el Centro de Informática de la Institución elaboran tres personas las cuales cumplen la siguiente estructura como muestra el cuadro 3.1:



Cuadro 3. 1 Estructura Interna del Centro de Informática

El Centro de Informática es el pilar fundamental para lograr la agilidad administrativa y de control de información existente en toda la Institución. Cuenta con una infraestructura de hardware repartida en todas las oficinas de cada uno de los Departamentos; además brinda servicio de tecnología de la información a los usuarios tanto académicos como administrativos, militares y civiles del plantel.

3.1.5 Características de los Sistemas y Ambiente de Tecnologías de Información



Cuadro 3. 2 Ambiente de Tecnologías del Centro de Informática

El *Jefe del Centro de Informática* realiza las siguientes funciones:

- Asiste técnicamente sobre instalaciones, actualización, funcionamiento y mantenimiento preventivo de hardware, software y redes de toda la unidad. Lleva un control de los recursos computacionales (hardware, software, redes y telecomunicaciones) que posee el COMIL Nº 10.
- Establece normas de seguridad de uso de, computadoras, redes y software de la unidad. Realizando un Plan informático anual en coordinación con las autoridades de la Institución.
- Coordina con los jefes departamentales para la elaboración del Plan de Mantenimiento preventivo y correctivo de los recursos computacionales y de redes de la unidad y también coordina las

actividades de capacitación profesional del personal del Centro de Informática.

- Asesora y mantiene actualizada la página web interactiva del COMIL Nº 10 para consulta de todas las actividades de la Institución. Coordina la adquisición de equipos informáticos y técnicos que la Institución requiera, formando parte de la comisión de adquisiciones.
- Mantiene actualizados los respaldos de la información que generan los sistemas académicos y administrativos de la Institución. Ejecuta y supervisa estrategias de respaldos y recuperación de la base de datos aplicando también la definición de procedimientos de contingencia.
- Administra y supervisa los sistemas operativos y servidores relacionados.
- Monitorea y optimiza el funcionamiento y rendimiento de las bases de datos.
- Administra usuarios y roles a nivel de bases de datos acorde a los requerimientos de las aplicaciones y asigna permisos para la utilización de la base de datos.

El *Administrador de Redes y Telecomunicaciones* realiza las siguientes funciones:

- Asiste técnicamente sobre instalaciones, actualización, funcionamiento y mantenimiento preventivo de las redes de toda la unidad.
- Revisa y mantiene las cuentas de correo electrónico que dispone la Institución y brinda el servicio al personal que lo solicite.

- Administra las redes y subredes del Colegio Militar, con el fin de agilitar los procesos en la Institución. Asesora a los usuarios de la Institución sobre la correcta utilización de los equipos e información procesada.
- Brinda soporte técnico a los usuarios de la red que intervienen en todos los sistemas académicos, administrativos, financieros. Instala y ejecuta las normas de seguridad en la utilización de los sistemas y paquetes educativos utilizados en la red.
- Establece controles de entrada y salida de información que requieren y emiten los sistemas de información del COMIL Nº 10. Ejecuta y supervisa el mantenimiento a los servicios de comunicación de datos (Internet, mensajería).
- Diseña, gestiona y ejecuta el mantenimiento a las redes de ordenadores, tanto física (redes de acceso, inalámbricas ópticas), lógicas (protocolos, arquitecturas), utilizando los avances tecnológicos en el área.

El *Administrador de Hardware* realiza las siguientes funciones:

- Asiste técnicamente sobre instalaciones, actualización, funcionamiento y mantenimiento preventivo de hardware de las dependencias administrativas del COMIL Nº 10.
- Realiza el mantenimiento preventivo de los computadores de los laboratorios de computación y del personal administrativo en coordinación con el Jefe del Centro de Informática.
- Lleva un registro KARDEX de las computadoras de la Institución y lleva un registro de control diario de los equipos asignados.

- Localiza y corrige fallas de funcionamiento de hardware y software, configura equipos, detecta y elimina virus informáticos. Instala equipos, dispositivos y verifica su correcto funcionamiento.
- Instruye a usuarios sobre la operación y manejo de equipos y paquetes informáticos. Instala y mantiene aplicaciones, sistemas operativos y paquetes informáticos.
- Elabora lista de insumos, materiales, repuestos y herramientas necesarias para las labores de mantenimiento del hardware y software.

3.2 Auditoría de la Gestión de TI

3.2.1 Selección de los Procesos y Escenarios hacer Auditados

Para tener un criterio del marco de trabajo se sigue un estándar de auditoría general y los criterios del modelo de COBIT que proporcionan un marco de referencia y de trabajo estandarizado, que involucran documentos con temas clasificados a través de dominios, procesos y actividades.

Para identificar las áreas que serán auditadas, se usará una matriz de riesgos y encuestas para trabajar con ellas durante todo el proceso de pre auditoría y que sirven para hacer el análisis de prioridades que dará información de fuentes directas como la Dirección, la Administración de TI y usuarios finales, para hacer la priorización y la auditoría informática.

3.2.2 Proceso de Recopilación de Información para la Selección de Prioridades y Riesgos

Antes de empezar a recopilar la información se ha preparado al personal y a los directivos para entender lo que significa aplicar el estándar COBIT en la Institución, que beneficios se pueden obtener, cuales son las áreas en las que se enfocara el estudio general y cual es el proceso que se seguirá para seleccionar las actividades a ser auditadas.

Este estándar no solo se puede usar como herramientas de auditoría sino también como una buena práctica de control periódico, seguimiento y evaluación de riesgos en el área de TI. De esta manera se han ido introduciendo los términos que se usan para evaluar la situación del Departamento Informático.

Se empleará técnicas de recopilación de evidencias que se detallan a continuación:

- Revisión de las estructuras organizacionales de sistemas de información.
- Revisión de planes de TI, documentos que inician el desarrollo del sistema, historia de cambios a programas, manuales de usuario, especificaciones de bases de datos, listados de programas.
- Entrevistas con el personal apropiado, las cuales deben tener una naturaleza de descubrimiento no de acusatoria.
- Observación de operaciones y actuación de empleados.

- Auto documentación, el auditor prepara narrativas en base a su observación, cuestionarios de entrevistas realizados y aplicación de técnicas de muestreo pruebas (de cumplimiento o sustantivas).
- Checklist, en la conducción del caso de estudio para comprobar las tareas implementadas en el Centro de Informática.
- Matriz RACI, para delimitar las actividades y los responsables en la conducción del caso de estudio.
- Tabla de observación de tareas, para revisar las políticas y planes existentes de tecnología.
- Hallazgos encontrados, los resultados encontrados en el diagnóstico de análisis de resultados.

Se utilizó una matriz de riesgos Implementada por ISACA, Cobit Implementation Tool Set indicado en la tabla 3.1, que permite realizar el análisis de riesgos y en base a ese análisis priorizar los objetivos de control que serán evaluados ya que resultaría demasiado laborioso y muy extenso el aplicar la auditoría en todos los procesos y objetivos de control que comprende el estándar de COBIT, por lo que para este caso se ha decidido realizar una selección de los procesos que en base a las entrevistas realizadas y a los resultados obtenidos se consideraron los objetivos de control más importantes. La información se recopiló en base a entrevistas y encuestas que se las puede ver en la sección de anexos como *Anexo B*.

3.2.2.1 Matriz de Riesgos

Esta matriz ayuda a identificar y realizar un análisis exhaustivo de los riesgos, permitiendo determinar los objetivos de control que serán considerados para la evaluación.

Se ha tomado como referencia la matriz de evaluación del riesgo de ISACA de la tabla 3.1. Para llenar este formulario se ha tomado en cuenta las respuestas emitidas por los encuestados y entrevistados, con esta información se ha realizado un resumen que ayuda a calificar las actividades de acuerdo al orden de importancia y de riesgo.

Unificando dicha información y tabulando por cada uno de los Dominios de COBIT, se selecciona los que resulten con mayor grado de importancia y que pueden ser aplicados en la Institución.

Cuyo enfoque principal se centra en el nivel de riesgo que el encuestado identifica en cada una de las actividades y del análisis realizado en cada evaluación, mediante el levantamiento de información del formulario:

- En la sección titulada **Importancia** se puede tener resultados como:

  - Menos importante **1**

  - Más importante **5**

- El segundo parámetro es el **Funcionamiento** en el que se identifica cual es el nivel de funcionamiento actual, puede tener resultados como:

  - No se realiza **1**

  - Se realiza **5**

- En la sección de **No se aplica** se señala con una **X** los procesos de control que se determinen no funcionales.
- La sección de **Quién lo realiza** permite identificar específicamente las actividades que corresponden al Departamento Informático, para lo cual existen varias alternativas:

  - Puede ser realizado por el **Departamento de Sistemas**

  - Puede ser realizado por **Otros** dentro de la misma Institución.

  - Por **Externos** como outsourcing o contratados para tareas específicas

  - **No conoce** puede existir la posibilidad de que la persona consultada no esté al tanto de quien es el encargado.

- El siguiente ítem trata de identificar si las actividades son controladas y formalizadas:

  - **Auditado** o **No** si se ha realizado anteriormente alguna evaluación.

  - A través de documentos aprobados por la administración de la Institución, a estos controles se los llama: **Formalizado** o **No**.
- El siguiente parámetro indica quien es el **Responsable**, es decir cual es la persona encargada de las tareas relacionadas con la actividad consultada.
- Por último se tiene la sección de **IMPACTO** en la cual se busca medir el riesgo y se han planteado las siguientes posibilidades:

  - **Alto**

  - **Medio**

  - **Bajo**

- **Inmaterial**

- **No esta seguro**

La información levantada de esta matriz será tomada como parte principal de la selección de las áreas auditables.

En el *Anexo A* se presenta un cuadro resumen de la Evaluación Informática, que proporciona una indicación por proceso y dominio de TI aplicados en el proyecto.

Tabla 3. 1 Matriz de Riesgos

EVALUACIÓN DEL RIESGO																
RIESGO			Calificar de 1 a 5 según lo siguiente: **Importancia**: **1** menos importante, **5** mas importante **Funcionamiento: 1** no se realiza, **5** se realiza **No se aplica: X** no se aplica **Auditado: Si** - se esta auditando frecuentemente, **No** - no se realiza auditoría **Formalizado**: Existe un contrato de servicio o se tiene claramente documentado el proceso (**SI** o **No**) **Responsable**: Nombre del responsable (o No sabe) **Impacto:** Medición del riesgo Alto, Medio, Bajo, Inmaterial, No esta seguro	**Responsable que lo realiza**							**IMPACTO**				
Importancia	**Funcionamiento**	**No se aplica**		**Departamento de Sistemas**	**Otros**	**Externos**	**No conoce**	**Auditado**	**Formalizado**	**Responsable**	**Alto**	**Medio**	**Bajo**	**Inmaterial**	**No esta seguro**
			PROCESOS DE IT												
			PLANIFICACION Y ORGANIZACIÓN												
5	5		PO1 Definir un Plan Estratégico de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas			Alto		
5	1		PO1.1 - Administración del valor de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas			Medio		
5	5		PO1.2 - Alineación de TI con el negocio		Otros			No	Si	Dirección			Alto		
5	5		PO1.3 - Evaluación de desempeño y la capacidad actual		Otros			No	Si	Equipo de Evaluación			Alto		
5	1		PO1.4 - Plan Estratégico de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas			Alto		
5	1		PO1.5 – Planes tácticos de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas				No esta seguro	
5	5		PO1.6 - Administración del Portafolio de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas			Medio		
1	1	X	PO2 Definir la Arquitectura de la Información					No	No					Inmaterial	
1	1	X	PO3 Determinar la Dirección Tecnológica					No	No					Inmaterial	
5	5		PO4 Definir la Organización y las Relaciones de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas			Alto		
5	1		PO4.1 - Marco de trabajo de procesos de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas			Medio		
5	5		PO4.2 - Comité Estratégico de TI	Departamento de Sistemas				No	No	Jefe de Sistemas			Medio		
5	5		PO4.3 - Comité Directivo de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas			Medio		
5	5		PO4.4 - Ubicación organizacional de la Función de TI		Otros			No	Si	Administración			Alto		
5	5		PO4.5 - Estructura Organizacional de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas			Alto		

Tabla 3. 1 Matriz de Riesgos (Continuación)

RIESGO			PROCESOS DE IT	Responsable que lo realiza				Auditado	Formalizado	Responsable	IMPACTO				
Importancia	Funcionamiento	No se aplica		Departamento de Sistemas	Otros	Externos	No conoce				Alto	Medio	Bajo	Inmaterial	No esta seguro
5	5		PO4.6 - Establecer las funciones y responsabilidades	Departamento de Sistemas				No	Si	Jefe de Sistemas	Alto				
5	5		PO4.7 - La responsabilidad de control de calidad de TI	Departamento de Sistemas				No	Si	Ingeniero de Soporte	Alto				
5	5		PO4.8 - Responsabilidad sobre el riesgo, la seguridad y el cumplimiento	Departamento de Sistemas				No	Si	Jefe de Sistemas	Alto				
5	5		PO4.9 - Propiedad de los sistemas y datos	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			
5	5		PO4.10 - Supervisión		Otros			No	Si	Jefe de Sistemas		Medio			
5	5		PO4.11 - La segregación de funciones				No conoce	No	No	No sabe					No esta seguro
5	5		PO4.12 - Descripción del cargo para el personal de la Informática	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			
5	5		PO4.13 - Personal clave de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas	Alto				
5	5		PO4.14 - Procedimientos y políticas para personal contratado		Otros			No	Si	Administración		Medio			
5	5		PO4.15 - Relaciones		Otros			No	Si	Administración		Medio			
5	5		PO5 Administrar la inversión en TI		Otros			No	Si	Jefe Financiero	Alto				
5	5		PO5.1 - Marco de Trabajo para la Administración Financiera		Otros			No	Si	Jefe Financiero		Medio			
5	5		PO5.2 - Prioridades dentro del presupuesto de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			
5	5		PO5.3 - Proceso Presupuestal	Departamento de Sistemas				No	Si	Jefe de Sistemas	Alto				
5	5		PO5.4 - Administración de Costes de TI		Otros			No	Si	Jefe Financiero	Alto				
5	1		PO5.5 - Administración de Beneficios				No conoce	No	No	No sabe					No esta seguro
5	5		PO6 Comunicar las aspiraciones y la dirección de la gerencia		Otros			No	Si	Dirección		Medio			
5	5		PO6.1 - Ambiente de políticas y de control		Otros			No	Si	Dirección		Medio			
5	5		PO6.2 - Riesgo corporativo y marco de referencia de control interno de TI	Departamento de Sistemas				No	No	Jefe de Sistemas	Alto				
5	5		PO6.3 - Administración de políticas de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			

Tabla 3. 1 Matriz de Riesgos (Continuación)

RIESGO			PROCESOS DE IT	Responsable que lo realiza				Auditado	Formalizado	Responsable	IMPACTO				
Importancia	Funcionamiento	No se aplica		Departamento de Sistemas	Otros	Externos	No conoce				Alto	Medio	Bajo	Inmaterial	No esta seguro
5	5		PO6.4 - Implantación de Políticas de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			
5	5		PO6.5 - Comunicación de los objetivos y la dirección de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			
1	1	X	PO7 Administrar los Recursos Humanos de TI					No	No					Inmaterial	
1	1	X	PO8 Administrar la calidad					No	No					Inmaterial	
5	5		PO9 Evaluar y Administrar los Riesgos de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas	Alto				
5	1		PO9.1 - Marco de Trabajo de Administración de Riesgos	Departamento de Sistemas				No	SI	Jefe de Sistemas	Alto				
5	1		PO9.2 - Establecimiento del contexto del riesgo	Departamento de Sistemas				No	Si	Jefe de Sistemas	Alto				
5	5		PO9.3 - Identificación de eventos	Departamento de Sistemas				No	No	Jefe de Sistemas	Alto				
5	1		PO9.4 - Evaluación de riesgos de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas	Alto				
5	1		PO9.5 - Respuesta a los riesgos	Departamento de Sistemas				No	Si	Jefe de Sistemas	Alto				
5	1		PO9.6 - Mantenimiento y monitoreo de un plan de acción de riesgos	Departamento de Sistemas				No	Si	Jefe de Sistemas	Alto				
1	1	X	PO10 Administrar Proyectos					No	No					Inmaterial	
			ADQUISICION E IMPLEMENTACION												
1	1	X	AI1 Identificar Soluciones Automatizadas					No	No					Inmaterial	
5	5		AI2 Adquirir y Mantener Software Aplicativo	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			
5	1		AI2.1 - Diseño de alto nivel	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			
5	5		AI2.2 - Diseño Detallado	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			
5	1		AI2.3 - Control y posibilidad de auditar las Aplicaciones	Departamento de Sistemas				No	Si	Jefe de Sistemas	Alto				
5	5		AI2.4 - Seguridad y disponibilidad de las aplicaciones	Departamento de Sistemas				No	Si	Ingeniero de Soporte		Bajo			
5	5		AI2.5 - Configuración e implementación de software de aplicativo adquirido	Departamento de Sistemas				No	Si	Ingeniero de Soporte	Alto				

Tabla 3. 1 Matriz de Riesgos (Continuación)

RIESGO			PROCESOS DE IT	Responsable que lo realiza				Auditado	Formalizado	Responsable	IMPACTO				
Importancia	Funcionamiento	No se aplica		Departamento de Sistemas	Otros	Externos	No conoce				Alto	Medio	Bajo	Inmaterial	No esta seguro
5	1		AI2.6 - Actualizaciones importantes en sistemas existentes	Departamento de Sistemas				No	Si	Ingeniero de Soporte		Medio			
5	5		AI2.7 - Desarrollo de software aplicativo	Externos				No	Si	Proveedor		Medio			
5	5		AI2.8 - Aseguramiento de la calidad del Software	Departamento de Sistemas				No	No	Jefe de Sistemas		Alto			
5	5		AI2.9 - Administración de los requerimientos de aplicaciones	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			
5	5		AI2.10 - Mantenimiento de software aplicativo	Externos				No	Si	Proveedor		Medio			
5	5		AI3 Adquirir y Mantener Infraestructura Tecnológica	Departamento de Sistemas				No	Si	Jefe de Sistemas		Alto			
5	5		AI3.1 - Plan de adquisición de infraestructura tecnológica	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			
5	5		AI3.2 - Protección y disponibilidad del recurso de infraestructura	Departamento de Sistemas				No	Si	Jefe de Sistemas		Alto			
5	5		AI3.3 - Mantenimiento de la infraestructura	Departamento de Sistemas				No	Si	Jefe de Sistemas		Alto			
5	1		AI3.4 - Ambiente de prueba de factibilidad	No conoce				No	No	No sabe					No esta seguro
5	5		AI4 Facilitar la operación y el uso	Departamento de Sistemas				No	Si	Ingeniero de Soporte			Bajo		
5	1		AI4.1 - Plan para soluciones de operación	Departamento de Sistemas				No	No	Ingeniero de Soporte		Alto			
5	5		AI4.2 - Transferencia de conocimiento a la gerencia del negocio	Departamento de Sistemas				No	Si	Ingeniero de Soporte			Bajo		
5	5		AI4.3 - Transferencia de conocimiento a usuarios finales	Departamento de Sistemas				No	Si	Proveedor			Bajo		
5	5		AI4.4 - Transferencia de conocimiento al personal de operaciones y soporte	Externos				No	Si	Proveedor			Bajo		
1	1	X	AI5 Adquirir recursos de TI					No	No					Inmaterial	
1	1	X	AI6 Administrar cambios					No	No					Inmaterial	
1	1	X	AI7 Instalar y acreditar soluciones y cambios					No	No					Inmaterial	

Tabla 3. 1 Matriz de Riesgos (Continuación)

RIESGO			PROCESOS DE IT	Responsable que lo realiza				Auditado	Formalizado	Responsable	IMPACTO				
Importancia	Funcionamiento	No se aplica		Departamento de Sistemas	Otros	Externos	No conoce				Alto	Medio	Bajo	Inmaterial	No esta seguro
			ENTREGA Y SOPORTE												
1	1	X	DS1 Definir y administrar los niveles de servicio					No	No					Inmaterial	
5	5		DS2 Administrar los servicios de terceros	Departamento de Sistemas				No	Si	Jefe de Sistemas			Medio		
5	5		DS2.1 - Identificación de todas las relaciones con proveedores	Departamento de Sistemas				No	Si	Jefe de Sistemas			Medio		
5	5		DS2.2 - Gestión de relaciones con proveedores	Departamento de Sistemas				No	Si	Jefe de Sistemas			Medio		
5	5		DS2.3 - Administración de riesgos del proveedor	Departamento de Sistemas				No	No	Jefe de Sistemas			Alto		
5	5		DS2.4 - Monitoreo del desempeño del proveedor	Departamento de Sistemas				No	Si	Jefe de Sistemas			Medio		
1	1	X	DS3 Administrar el desempeño y la capacidad					No	No					Inmaterial	
1	1	X	DS4 Garantizar la continuidad del servicio					No	No					Inmaterial	
1	1	X	DS5 Garantizar la seguridad de los sistemas					No	No					Inmaterial	
1	1	X	DS6 Identificar y asignar costos					No	No					Inmaterial	
5	5		DS7 Educar y capacitar a los usuarios	Departamento de Sistemas				No	Si	Ingeniero de Soporte			Alto		
5	5		DS7.1 - Identificación de necesidades de entrenamiento y educación	Departamento de Sistemas				No	Si	Jefe de Sistemas			Alto		
5	5		DS7.2 - Impartición de entrenamiento y educación	Departamento de Sistemas				No	Si	Ingeniero de Soporte			Medio		
5	1		DS7.3 - Evaluación del entrenamiento recibido		Otros			No	No	Equipo de Evaluación			Alto		
1	1	X	DS8 Administrar la mesa de servicio y los incidentes					No	No					Inmaterial	
1	1	X	DS9 Administrar la Configuración					No	No					Inmaterial	
5	5		DS10 Administrar los problemas	Departamento de Sistemas				No	Si	Ingeniero de Soporte			Medio		
5	5		DS10.1 - Identificación y clasificación de problemas	Departamento de Sistemas				No	Si	Ingeniero de Soporte			Alto		
5	5		DS10.2 - Rastreo y resolución de problemas	Departamento de Sistemas				No	Si	Ingeniero de Soporte			Medio		

Tabla 3. 1 Matriz de Riesgos (Continuación)

RIESGO			PROCESOS DE IT	Responsable que lo realiza				Auditado	Formalizado	Responsable	IMPACTO				
Importancia	Funcionamiento	No se aplica		Departamento de Sistemas	Otros	Externos	No conoce				Alto	Medio	Bajo	Inmaterial	No esta seguro
5	5		DS10.3 - Cierre de problemas	Departamento de Sistemas				No	Si	Ingeniero de Soporte		Medio			
5	1		DS10.4 - Integración de las administraciones de cambios, configuración y problemas	No conoce				No	No	No sabe					No esta seguro
1	1	X	DS11 Administrar los datos					No	No					Inmaterial	
1	1	X	DS12 Administrar el ambiente físico					No	No					Inmaterial	
1	1	X	DS13 Administrar las operaciones					No	No					Inmaterial	
			MONITOREAR Y EVALUAR												
5	5		ME1 Monitorear y evaluar el desempeño de TI	Departamento de Sistemas				No	Si	Jefe de Sistemas		Alto			
5	5		ME1.1 - Enfoque del Monitoreo	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			
5	5		ME1.2 - Definición y recolección de datos de monitoreo	Departamento de Sistemas				No	Si	Jefe de Sistemas		Alto			
5	1		ME1.3 - Método de monitoreo	No conoce				No	No	No sabe		Alto			
5	5		ME1.4 - Evaluación del desempeño	Otros				No	Si	Equipo de Evaluación		Alto			
5	5		ME1.5 - Reportes al Consejo Directivo y a Ejecutivos	Departamento de Sistemas				No	Si	Jefe de Sistemas		Medio			
5	5		ME1.6 - Acciones Correctivas	Departamento de Sistemas				No	Si	Jefe de Sistemas		Alto			
1	1	X	ME2 Monitorear y evaluar el control interno					No	No					Inmaterial	
1	1	X	ME3 Garantizar el cumplimiento con requerimientos externos					No	No					Inmaterial	
1	1	X	ME4 Proporcionar Gobierno de TI					No	No					Inmaterial	

3.2.2.2 Resumen de los Procesos Seleccionados para el Análisis

Luego de realizar la revisión exhaustiva del análisis de riesgos con el Jefe del Centro de Informática de la Institución y el análisis de priorización de los procesos sujetos a la evaluación, se obtiene como resultado que la calificación a cada proceso se ha valorado en base a los parámetros de su importancia, funcionalidad, formalidad, responsabilidad y el impacto que tendría como riesgo a los procesos en el ámbito de la Institución educativa obtenidos por las entrevistas y encuestas que se encuentran en el *Anexo B*.

Se puede observar en el análisis de la matriz de riesgos que no se ha seleccionado a los procesos que obtuvieron calificación ***1*** en la importancia, con respuesta ***No*** al proceso que no ha sido formalizado y en el impacto a los procesos que se hayan valorado como ***inmaterial***, de igual manera se ha considerado para mostrar un resumen comprensible de la selección otros parámetros como Responsable que lo realiza especificando los procesos que se encarga el ***Departamento Informático*** y el ***Responsable***.

En base a los resultados analizados se ha contestado con una ***X*** a los procesos que no se aplicarán en la evaluación del COMIL Nº 10.

Por último los procesos que se aplican en la evaluación son los que se han calificado por su importancia con el valor de **5** y el impacto reflejado en base al análisis ***alto***, ***medio*** o ***bajo***.

A continuación se indican los procesos que se han considerado para la evaluación del Centro de Informática de la Institución, especificando los objetivos de control de cada uno de ellos:

PLANIFICACIÓN Y ORGANIZACIÓN

PO1: Definir un Plan Estratégico de TI

PO4: Definir la Organización y las Relaciones de TI

PO5: Administrar la Inversión en TI

PO6: Comunicar las Aspiraciones y la Dirección de la Gerencia

PO9: Evaluar y Administrar los Riesgos de TI

ADQUISICIÓN E IMPLEMENTACIÓN

AI2: Adquirir y Mantener Software Aplicativo

AI3: Adquirir y Mantener Infraestructura Tecnológica

AI4: Facilitar la Operación y el Uso

ENTREGA Y SOPORTE

DS2: Administrar los Servicios de Terceros

DS7: Educar y Capacitar a los Usuarios

DS10: Administrar los Problemas

MONITOREAR Y EVALUAR

ME1: Monitorear y Evaluar el Desempeño de TI

3.3 Investigación de Campo

La investigación de campo ayuda a determinar la importancia, la funcionalidad, y los controles que se están realizando en los procesos. En esta etapa se utiliza la matriz de Investigación de Campo ver en la tabla 3.2 que se ha desarrollado para la Evaluación Técnica Informática del COMIL Nº 10 ABDÓN CALDERÓN. Este tipo de formularios lo que pretende es ayudar a evaluar y medir el nivel de madurez en el que se encuentra el Departamento Informático y está fundamentada en las directrices de auditoría planteadas en COBIT, cuyo propósito es contar con una estructura sencilla para auditar y evaluar los controles.

Este estándar no sólo se puede usar como herramienta de auditoría sino también como una buena práctica de control periódico, seguimiento y evaluación de riesgos en el área de TI. La recopilación de esta información se enmarca en:

3.3.1 Control Interno

Evalúa los procesos que se encuentran formalmente documentados, afirma la posibilidad planteada de que exista una documentación formal aprobada y difundida en la Institución, sobre las actividades realizadas, para tal efecto el encuestado tiene tres opciones a elegir:

- Documentado
- No documentado
- No esta seguro

3.3.2 Desempeño

Evalúa el desempeño identificando los niveles de resultados que se obtiene de las actividades realizadas para lo cual se tiene las siguientes opciones:

- Excelente
- Muy Bueno
- Satisfactorio
- Pobre
- No se aplica

3.3.3 Evaluación

La evaluación se enfoca en requerimientos para lograr una gestión y un control adecuado de TI permitiendo medir en un nivel alto, de manera justa, transparente, repetible y comparable. Para ello se fundamenta en las siguientes puntualizaciones:

- **Pruebas realizadas:** Es aplicado para la valoración del cumplimiento para las pruebas en cada proceso.
- **Documento de respaldo:** En esta opción se realiza el registro de las evidencias presentadas, es decir los documentos que fueron oficiales y que estuvieron disponibles en la Institución.
- **Resultados:** Son las conclusiones a las que se ha llegado luego de la auditoría previa.

En los siguientes puntos se detalla la investigación de campo para la evaluación informática de los objetivos de control de los procesos relacionados para el análisis según la propuesta de COBIT.

3.3.4 Procesos del Dominio de Planificación y Organización

3.3.4.1 Evaluación de los controles para el proceso PO1 Definir un Plan Estratégico de TI

En la tabla 3.2 se muestran los resultados de la evaluación de los controles para el Proceso PO1.

Tabla 3. 2 Evaluación de los controles para el Proceso PO1

CONTROL INTERNO			**Control Interno:** Los procesos se encuentran documentados o no documentados, no esta seguro **Desempeño:** Categorización de la evaluación si es excelente, muy bueno, satisfactorio, pobre o no se aplica. **Pruebas Realizadas:** Descripción de las pruebas realizadas **Documento de Respaldo:** Evidencias que respaldan a la evaluación **Resultados:** Resultado de la evaluación de los controles aplicados en la auditoría	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro	PROCESOS DE IT	Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
			PLANIFICACIÓN Y ORGANIZACIÓN								
Documentado			PO1 Definir un Plan Estratégico de TI	Satisfactorio					Entrevista al Jefe del Centro de Informática	Plan Informático de Organización 2008-2009	El documento de planeación del Departamento Informático satisface poco a los requerimientos de la Institución

Tabla 3. 2 Evaluación de los controles para el Proceso PO1 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			PO1.1 - Administración del valor de TI	Muy Bueno					Pedido de todos los documentos de planeación existentes	Instructivos y Normas del Comando de Educación y Doctrina del Ejército Ecuatoriano: Centro de Informática (CDI) y Secciones Informáticas (SEI). Plan Informático de Organización 2008-2009. Plan anual de inversiones. Lineamientos y Políticas de Planificación y Ejecución de la Programación Anual de la Política Pública 2012-2013. Plan de mantenimiento de computadoras. Normas y Formatos de la Secretaría Nacional de Planificación y Desarrollo (Senplades).	Existe documentos de planeación pero no son elaborados por el Departamento Informático del establecimiento a excepción del plan informático anual y el de mantenimiento de hardware
Documentado			PO1.2 - Alineación de TI con el negocio	Pobre					Entrevista con las autoridades para verificar que las estrategias de la Institución estén integradas con la Tecnología de Información	Plan Estratégico Institucional	Las estrategias de la Institución no están relacionadas con las TI

Tabla 3. 2 Evaluación de los controles para el Proceso PO1 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
No esta seguro			PO1.3 - Evaluación de desempeño y la capacidad actual	Pobre					Evaluación de los planes existentes y de sistemas actuales	Evaluación al personal y a la gerencia	Los planes existente y los sistemas de información académico y administrativo favorece poco a los objetivos de la Institución
Documentado			PO1.4 - Plan Estratégico de TI	Muy Bueno					Revisión de documentos que soporten el Plan estratégico Informático	Plan Informático de Organización 2008-2009	El plan estratégico Informático contribuye a los objetivos estratégicos de la Institución
Documentado			PO1.5 – Planes tácticos de TI	Muy Bueno					Revisión de la gestión de requerimientos de las Ti	Plan Informático de Organización 2008-2009, Plan de mantenimiento de hardware, Plan de Seguridad de la Información	Se administra de forma continua los planes informáticos sin embargo no se lleva de manera ágil los procedimientos recomendados
Documentado			PO1.6 - Administración del Portafolio de TI	Muy Bueno					Revisión de programas de inversión y presupuesto de TI	Plan anual de Trabajo, Plan anual de inversiones	Tienen un programa de presupuesto acorde a los requerimientos del alumnado y en base a las políticas establecidas por el Comando de Educación y Doctrina del Ejército y Senplades

3.3.4.2 Evaluación de los controles para el proceso PO4 Definir la Organización y las Relaciones de TI

En la tabla 3.3 se muestran los resultados de la evaluación de los controles para el Proceso PO4.

Tabla 3. 3 Evaluación de los controles para el Proceso PO4

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			PO4 Definir la Organización y las Relaciones de TI	Muy Bueno					Entrevista con Jefe del Centro de Informática	Plan Informático de Organización 2008-2009	Las relaciones con las otras direcciones departamentales es la adecuada como para identificar los problemas y entender los temas de Tecnología relacionados pero se debe mejorar algunos procesos
		No esta seguro	PO4.1 - Marco de trabajo de procesos de TI	Pobre					Entrevista con Jefe del Centro de Informática	No existe documentos	Se tiene establecido un marco de referencia de Normas de Senplades para cumplir los objetivos y adecuar las metas a las circunstancias cambiantes sin embargo están en proceso de transición por recientes disposiciones de dicha entidad, para su cumplimiento aun no se formaliza en el Departamento

Tabla 3. 3 Evaluación de los controles para el Proceso PO4 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
No documentado			PO4.2 - Comité Estratégico de TI	Pobre					Entrevista con Jefe del Centro de Informática	No existe documentación	No existe un comité estratégico del Departamento Informático solo existe de la Institución y se realizan evaluaciones continuas del personal, actuando coherentemente con estas evaluaciones
No documentado			PO4.3 - Comité Directivo de TI	Pobre					Entrevista con el Comité de direccionamiento de TI y sus actividades	No existe documentación	No existe comité de planeamiento de TI que supervise la función de TI y sus actividades. La resolución de artículos de acción a nivel Institucional lo realiza el Comité Directivo de la Institución que esta formada por los Jefes Departamentales
Documentado			PO4.4 - Ubicación organizacional de la Función de TI	Muy Bueno					Pedido del Organigrama de la Institución	Organigrama Funcional	Se tiene independencia y un grado de autoridad suficiente para utilizar
Documentado			PO4.5 - Estructura Organizacional de TI	Satisfactorio					Pedido de la Estructura interna del Centro de Informática	Estructura interna del Departamento de TI	Se tiene una estructura interna suficiente para la gestión tecnológica en el establecimiento
Documentado			PO4.6 - Establecer las funciones y responsabilidades	Muy Bueno					Entrevista al personal del Centro de Informática	Acta de Responsabilidad de la Planificación	La Dirección de TI esta enterada de sus roles y responsabilidades

Tabla 3. 3 Evaluación de los controles para el Proceso PO4 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
No esta seguro			PO4.7 - La responsabilidad de control de calidad de TI	Pobre					Entrevista al Jefe del Centro de Informática	Metodología de pruebas del Instructivo del Comando de Educación y Doctrina del Ejército	El Jefe del Centro de Informática junto al Administrador de hardware se encarga del control de calidad del software, pero no se tiene claro la responsabilidad de las actividades del administrador de Redes, Telecomunicaciones y Seguridades. El grupo de QA no aplica de manera consistente la metodología para que satisfagan los requerimientos de la Institución
Documentado			PO4.8 - Responsabilidad sobre el riesgo, la seguridad y el cumplimiento	Pobre					Revisión de responsabilidades de los sistemas operativos centrales y los sistemas de aplicación	Plan Informático de Organización 2008-2009	Existe un responsable de seguridad lógica, sin embargo la seguridad física no tiene un encargado, excepto por la seguridad integral general de la Institución
Documentado			PO4.9 - Propiedad de los sistemas y datos	Pobre					Entrevista al personal del Centro de Informática	Inventario de Estados Internos con Lista de activos asignados al personal	No se tiene un esquema para asegurar que las decisiones sobre los bienes recaigan a las personas correctas. La responsabilidad se da casi en su totalidad al grupo de operación. La jefatura informática maneja inventario a nivel de hardware y la adquisición de licencias esta en estudio para nuevo proyecto solamente para office y Windows

Tabla 3. 3 Evaluación de los controles para el Proceso PO4 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			PO4.10 - Supervisión	Muy Bueno					Descripciones del cargo que describan claramente la autoridad y responsabilidad	Instructivo para el funcionamiento de los Centros de Informática (CDI) y Secciones Informáticas (SEI) del Ejército Ecuatoriano	Se tiene implementado un esquema de supervisión de actividades y evaluación de personal. Los indicadores de gestión se los realiza según el instructivo del Comando de Educación y Doctrina del Ejército
Documentado			PO4.11 - La segregación de funciones	Satisfactorio					Análisis del organigrama solicitado	Plan Informático de Organización 2008-2009	En la especificación de Puestos de Trabajo se establece la división de roles y responsabilidades asegurando de que el personal realice solo tareas autorizadas
Documentado			PO4.12 - Descripción del cargo para el personal de la Informática	Muy Bueno					Pedido del documento de descripción del cargo del Centro de Informática	Plan Informático de Organización 2008-2009	Se tiene establecido las descripciones de los cargos en base a las disposiciones del Comando de Educación y Doctrina del Ejército correspondiente a la Administración de TI
Documentado			PO4.13 - Personal clave de TI	Muy Bueno					Pedido de lista de funciones de empleados del Centro de Informática	Plan Informático de Organización 2008-2009	Se tiene identificado claramente el personal clave para cada función de TI
Documentado			PO4.14 - Procedimientos y políticas para personal contratado	Muy Bueno					Políticas y procedimientos relacionados con el contrato de personal	Actualmente es manejado por el Estado a través del Sistema de Contratación Pública	No se tiene definido e implementado políticas y procedimientos para contratar las actividades de los consultores y otro personal contratado debido a que actualmente lo gestiona el Estado
No documentado			PO4.15 - Relaciones	Pobre					Entrevista al Personal Informático y Administrativo	No existe documentación	Se tiene implementado un buen esquema de comunicación aunque se requieren mejoras

3.3.4.3 Evaluación de los controles para el proceso PO5 Administrar la Inversión en TI

En la tabla 3.4 se muestran los resultados de la evaluación de los controles para el Proceso PO5.

Tabla 3. 4 Evaluación de los controles para el Proceso PO5

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			PO5 Administrar la inversión en TI	Muy Bueno					Pedido del presupuesto general de la Institución	Plan anual de inversiones	El presupuesto general de la Institución contempla las adquisiciones y los daños durante el año
Documentado			PO5.1 - Marco de Trabajo para la Administración Financiera	Muy Bueno					Entrevista con el Jefe Financiero	Presupuesto realizado por el Centro de Informática en base a los lineamientos y políticas de Planificación y Ejecución por parte del estado	El presupuesto es realizado por el Centro de Informática enviado al Departamento Financiero previa aprobación de Rectorado
Documentado			PO5.2 - Prioridades dentro del presupuesto de TI	Muy Bueno					Entrevista con el Jefe del Centro de Informática	Informe de Presupuesto anual y de necesidad Técnica en base a los lineamientos y políticas de Planificación y Ejecución de la Programación anual de la Política Pública 2012-2013, Plan anual de inversiones	El presupuesto es socializado y el Centro de Informática da prioridad a los gastos de mantenimiento, contempla los gastos de adquisición de hardware

Tabla 3. 4 Evaluación de los controles para el Proceso PO5 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			PO5.3 - Proceso Presupuestal	Muy Bueno					Pedido del presupuesto anual del Centro de Informática	Informe de Presupuesto anual del Centro de Informática y de necesidad Técnica	El presupuesto se lo realiza anualmente y en base a requerimientos necesarios con procedimientos del Estado como ordena la Senplades y el ministerio de Finanzas. El Centro de Informática envía el informe técnico al Departamento Administrativo y dicho Departamento se encarga de activar las compras
Documentado			PO5.4 - Administración de Costes de TI	Satisfactorio					Entrevista con el Jefe del Centro de Informática	Plan anual de Compras	Por políticas del Estado la gestión de costos lo realizan hasta el 15 de enero de cada año mediante un catálogo electrónico que se encuentra en el portal de compras públicas de la Institución
Documentado			PO5.5 - Administración de Beneficios	Satisfactorio					Entrevista con el Jefe del Centro de Informática	Normas de presentación de perfiles de proyectos de la Secretaría Nacional de Planificación y Desarrollo (Senplades)	Se gestiona con el Programa de inversión de TI que ordena el gobierno

3.3.4.4 Evaluación de los controles para el proceso PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia

En la tabla 3.5 se muestran los resultados de la evaluación de los controles para el Proceso PO6.

Tabla 3. 5 Evaluación de los controles para el Proceso PO6

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			PO6 Comunicar las aspiraciones y la dirección de la gerencia	Muy Bueno					Entrevista con el Rector	Reglamento interno de la Institución por el Comando de Educación y Doctrina del Ejército	La Dirección se preocupa por hacer conocer las políticas organizacionales, pero la comprensión y utilización por parte de toda la Institución no ha sido factible
Documentado			PO6.1 - Ambiente de políticas y de control	Muy Bueno					Entrevista con el Jefe del Centro de Informática	Lineamientos y políticas de planificación y ejecución de la programación anual de la política pública de la Fuerza Terrestre 2012-2013. Políticas para el funcionamiento de los centros de Informática (CDI) y secciones informáticas (SEI). Políticas de Educación Regular. Políticas de la Secretaría Nacional de Planificación y Desarrollo (Senplades). Políticas de Seguridad de la Información digital para el empleo en el Ejército Ecuatoriano	Existen varios documentos de políticas de control interno puestos en práctica y que ha sido suficientemente difundido dentro de la Institución para su programación

Tabla 3. 5 Evaluación de los controles para el Proceso PO6 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			PO6.2 - Riesgo corporativo y marco de referencia de control interno de TI	Muy Bueno					Entrevista con el Jefe del Centro de Informática	Plan de Seguridad de la Información	Se tiene una política de seguridad para la mitigación de riesgos, limitación de pérdidas y recuperación oportuna de información. Se han realizado actividades específicas bajo estas consideraciones
Documentado			PO6.3 - Administración de políticas de TI	Muy Bueno					Pedido de documentos de políticas para TI	Instructivo para el funcionamiento de los centros de informática (CDI) y secciones informáticas (SEI). Instructivo de políticas de Seguridad de la Información digital para el empleo en el Ejército Ecuatoriano	Existen políticas de TI que son dirigidas a los usuarios y a las funciones de los organismos de informática
Documentado			PO6.4 - Implantación de Políticas de TI	Pobre					Entrevista con el Jefe del Centro de Informática	Instructivo para el funcionamiento de los centros de informática (CDI) y secciones informáticas (SEI). Instructivo de políticas de Seguridad de la Información digital para el empleo en el Ejército Ecuatoriano	Existe varios marcos de referencia formal para realizar esta actividad en base a las disposiciones del Comando de Educación y Doctrina del Ejército mediante los instructivos del funcionamiento de los CDI y el instructivo de seguridad de la información, sin embargo las políticas implementadas por el Departamento Informático en la Institución no son documentadas
Documentado			PO6.5 - Comunicación de los objetivos y la dirección de TI	Muy Bueno					Comprobación del envío y recepción en la gestión Institucional que comunique las decisiones administrativas de TI	Documentos de Hojas de Control, Memorandos, Oficios y Ejemplares	La comunicación de los objetivos se los realiza mediante oficios se los conoce y se discute si es necesario. Muy poco se lo realiza por medio del correo electrónico de la Institución

3.3.4.5 Evaluación de los controles para el proceso PO9 Evaluar y Administrar los Riesgos de TI

En la tabla 3.6 se muestran los resultados de la evaluación de los controles para el Proceso PO9.

Tabla 3. 6 Evaluación de los controles para el Proceso PO9

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			PO9 Evaluar y Administrar los Riesgos de TI				Pobre		Entrevista con el Jefe del Centro de informática	Plan de Contingencia y Plan de Seguridad	Se tienen un mantenimiento de riesgos en base al plan de seguridad y contingencia pero no se realiza una gestión de riesgos y no se ha evaluado su costo
No esta seguro			PO9.1 - Marco de Trabajo de Administración de Riesgos					No se aplica	Pedido de gestión de riesgos de TI	No existe documentación	No se ha realizado Gestión de Riesgos de TI en la Institución
No esta seguro			PO9.2 - Establecimiento del contexto del riesgo				Pobre		Entrevista con el Jefe del Centro de informática	No existe documentación	No se tiene establecido evaluación de riesgos en el Departamento Informático excepto para la seguridad integral de la Institución
No documentado			PO9.3 - Identificación de eventos					No se aplica	Entrevista con el Jefe del Centro de informática	No existe documentación	No se tiene registro de riesgos
No documentado			PO9.4 - Evaluación de riesgos de TI				Pobre		Entrevista con el Jefe del Centro de informática	No existe documentación de riesgos identificados	Actualmente no se ha realizado una evaluación de costos de riesgos
Documentado			PO9.5 - Respuesta a los riesgos		Muy Bueno				Pedido de planes que mitiguen los riesgos	Plan de Seguridad de la Información, Plan de Contingencia	El plan de contingencia y seguridad contempla un proceso de respuesta a los riesgos con un buen diseño, el proceso de respuesta a riesgos identifica estrategias para mitigar los riesgos
Documentado			PO9.6 - Mantenimiento y monitoreo de un plan de acción de riesgos			Satisfactorio			Pedido de un Plan de Contingencia	Plan de Seguridad de la Información, Plan de Contingencia	Los planes establecen actividades de control recomendadas para asegurar el monitoreo y su ejecución

3.3.5 Procesos del Dominio de Adquisición e Implementación

3.3.5.1 Evaluación de los controles para el proceso AI2 Adquirir y Mantener Software Aplicativo

En la tabla 3.7 se muestran los resultados de la evaluación de los controles para el Proceso AI2.

Tabla 3. 7 Evaluación de los controles para el Proceso AI2

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
			ADQUISICION E IMPLEMENTACION								
Documentado			AI2 Adquirir y Mantener Software Aplicativo				Pobre		Entrevista con el Jefe del Centro de Informática	No existe el orden de trabajo de los proyectos, solamente tienen los sistemas con los que cuenta la Institución a base del Comando de Educación y Doctrina del Ejército según el Instructivo de los Centros de informática (CDI) y secciones informáticas (SEI)	El software aplicativo correspondiente al académico de la Institución fue adquirido en el 2001 y no se siguió ninguna metodología para evaluarlo y adquirirlo. Actualmente tienen un Sistema Integrado de la Fuerza Terrestre (SIFTE) el cual tiene varios subsistemas que gestiona a todas las entidades del ejército ecuatoriano siendo utilizados por el establecimiento doce subsistemas los mismos que son utilizados por el personal administrativo del COMIL 10.
	No Documentado		AI2.1 - Diseño de alto nivel				Pobre		Comprobación de que el software satisface los requerimientos del negocio	No existen documentos de diseño de alto nivel	El software aplicativo no cumple todos los requerimientos de la Institución

Tabla 3. 7 Evaluación de los controles para el Proceso AI2 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
No Documentado			AI2.2 - Diseño Detallado	Pobre					Pedido de aprobaciones de diseños, definición de requerimientos, interface, requerimientos de entrada y salida. Plan de pruebas y resultados del software de aplicación	No existe documentación	No existe documentación de desarrollo actualizada o completa del diseño
No Documentado			AI2.3 - Control y posibilidad de auditar las Aplicaciones	No se aplica					Pedido de documentos evaluados a las aplicaciones	No existe documentación de auditoría	No existe evaluación a las aplicaciones sin embargo tienen una propuesta de realizar un proyecto para unificar todos los sistemas académicos de los establecimientos militares y tener un solo sistema completo para todas las Instituciones militares ya que reconocen que el sistema actual es ineficiente
Documentado			AI2.4 - Seguridad y disponibilidad de las aplicaciones	Muy Bueno					Pedido de requerimientos de control interno, seguridad y disponibilidad	Plan de Seguridad	Se tiene un buen control de seguridad en la integridad de los datos
No Documentado			AI2.5 - Configuración e implementación de software de aplicativo adquirido	Pobre					Pedido de los requerimientos para la implantación del sistema y de la configuración base del sistema	No existe documentación de la configuración base para implementar el Sistema Integrado Educativo (SIE)	El Jefe del Centro de Informática manifiesta que el Sistema Integrado Educativo correspondiente al académico se ejecuta de manera normal pero reconoce que es un sistema que ha caducado y que están realizando estudios para cambiar de sistema

Tabla 3. 7 Evaluación de los controles para el Proceso AI2 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			AI2.6 - Actualizaciones importantes en sistemas existentes	Pobre					Entrevista con el Jefe del Centro de Informática	Lista de aplicaciones y sistemas actuales del Instructivo CDI y SEI	El sistema Integrado Educativo: académico, de secretaría y de colecturía fue adquirido desde 2001 sin actualizaciones, el portal web: http://www.comil10ac.edu.ec/ es el único sistema que tiene actualizaciones pero no se lleva un registro de cambios. El nuevo sistema del gobierno solo controla a nivel de gestión documental para docencia y empleados administrativos del COMIL 10
No Documentado			AI2.7 - Desarrollo de software aplicativo	No se aplica					Pedido de la metodología de desarrollo para los nuevos módulos del sistema	No existe documentos del ciclo de vida del sistema académico	El Centro de informática no ha seguido una metodología de desarrollo para el ciclo de vida del sistema integrado educativo
Documentado			AI2.8 - Aseguramiento de la calidad del Software	Muy Bueno					Entrevista con el Jefe del Centro de informática	Instructivo para el funcionamiento de los centros de informática (CDI) y secciones informáticas (SEI)	El aseguramiento de calidad de los sistemas se realiza por parte de TI y se hace un análisis del procedimiento. Se siguen algunos procesos para el cumplimiento de la norma Iso 9000 y 2000
No Documentado			AI2.9 - Administración de los requerimientos de aplicaciones	Pobre					Pedido de documentos para la realización de cambios	No existe diseño para la recopilación de datos	No se realiza un análisis de requerimientos para la entrada de datos
No Documentado			AI2.10 - Mantenimiento de software aplicativo	Pobre					Pedido del plan de mantenimiento del Sistema integrado educativo	No existe documentación sobre el plan de mantenimiento del sistema académico	El Centro de Informática no tiene un plan de mantenimiento para los sistemas y solamente se realiza actualizaciones del sistema web a nivel informativo

3.3.5.2 Evaluación de los controles para el proceso AI3 Adquirir y Mantener Infraestructura Tecnológica

En la tabla 3.8 se muestran los resultados de la evaluación de los controles para el Proceso AI3.

Tabla 3. 8 Evaluación de los controles para el Proceso AI3

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			AI3 Adquirir y Mantener Infraestructura Tecnológica	Muy Bueno					Entrevista al Jefe del Centro de Informática	Procedimiento para manejo de proyectos del Formato de la Secretaría Nacional de Planificación y Desarrollo (Senplades) mediante un Informe de Necesidad Técnica	Los resultados de cada proyecto son evaluados de acuerdo a los requerimientos que se recopilaron
Documentado			AI3.1 - Plan de adquisición de infraestructura tecnológica	Muy Bueno					Pedido del plan de adquisición de infraestructura tecnológica	Presupuesto realizado por el Centro de Informática. Plan Informático Anual	El único documento que contiene datos sobre la adquisición es el presupuesto realizado por el Centro de informática
Documentado			AI3.2 - Protección y disponibilidad del recurso de infraestructura	Muy Bueno					Pedido de planes de protección de la infraestructura	Plan de mantenimiento de equipos. Lista de Materiales para Mantenimiento Preventivo y Correctivo	Se realizan planes de protección de la infraestructura, mantenimiento preventivo y correctivo periódicamente

Tabla 3. 8 Evaluación de los controles para el Proceso AI3 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			AI3.3 - Mantenimiento de la infraestructura	Muy Bueno					Entrevista al personal del Centro de Informática sobre el mantenimiento y la protección de la infraestructura tecnológica	Plan de mantenimiento de equipos. Lista de Materiales para Mantenimiento Preventivo y Correctivo	El Centro de informática realiza el mantenimiento de hardware en los centros de computo, oficinas de la Institución y se las realiza en las fechas establecidas mediante el plan de mantenimiento, realizando un informe final
No esta seguro			AI3.4 - Ambiente de prueba de factibilidad	Pobre					Verificación de que las pruebas de funcionalidad, datos, configuración de software y hardware se realice	No existe documentación	Todos los sistemas tienen un proceso de pruebas los mismos que se realizan con los usuarios y existe una constancia de aprobación y aceptación

3.3.5.3 Evaluación de los controles para el proceso AI4 Facilitar la Operación y el Uso

En la tabla 3.9 se muestran los resultados de la evaluación de los controles para el Proceso AI4.

Tabla 3. 9 Evaluación de los controles para el Proceso AI4

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			AI4 Facilitar la operación y el uso	Pobre					Entrevista con el Jefe del Centro de Informática	Manual de Procesos	El único documento que contiene datos de procedimientos técnicos es el manual de procesos realizado por el Departamento Informático pero no hay un plan oficial
Documentado			AI4.1 - Plan para soluciones de operación	Pobre					Pedido de documentos técnicos sobre la capacidad de procedimientos de administración de usuarios y operativos	Manual de procesos	Solamente se tiene un manual de procesos pero el documento no es oficial
No Documentado			AI4.2 - Transferencia de conocimiento a la gerencia del negocio	Pobre					Entrevista con el Jefe del Centro de Informática	No existe documentación	Se sigue procedimientos para la capacitación sin embargo no se realiza de manera exhaustiva
Documentado			AI4.3 - Transferencia de conocimiento a usuarios finales	Pobre					Entrevista con el Administrador de hardware	Manual de Procesos	No existe un procedimiento eficiente para la capacitación de los usuarios
Documentado			AI4.4 - Transferencia de conocimiento al personal de operaciones y soporte	Pobre					Pedido de materiales de entrenamiento, manuales de procedimientos y manuales de usuario realizados por el Departamento Informático	Manual de Procesos	El manual de procesos que utilizan no satisface los requerimientos para que el personal de soporte técnico y de operaciones apoyen de manera efectiva

3.3.6 Procesos del Dominio de Entrega y Soporte

3.3.6.1 Evaluación de los controles para el proceso DS2 Administrar los Servicios de Terceros

En la tabla 3.10 se muestran los resultados de la evaluación de los controles para el Proceso DS2.

Tabla 3. 10 Evaluación de los controles para el Proceso DS2

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
			ENTREGA Y SOPORTE								
Documentado			DS2 Administrar los servicios de terceros			Satisfactorio			Entrevista con el Jefe del Centro de Informática	Portal de contrato de servicios por el Instituto Nacional de Contratación Pública	Se tiene los contratos registrados con las empresas proveedoras pero actualmente lo maneja el gobierno mediante el sistema nacional de Contratación Pública
Documentado			DS2.1 - Identificación de todas las relaciones con proveedores			Satisfactorio			Pedido de lista de contratos actuales de proveedores de servicio	Portal de Contrato de servicios por el Instituto Nacional de Contratación Pública	Se tiene establecido cual será el mecanismo de contacto entre los proveedores y la Institución actualmente lo maneja el gobierno

Tabla 3. 10 Evaluación de los controles para el Proceso DS2 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			DS2.2 - Gestión de relaciones con proveedores	Satisfactorio					Pedido de políticas de TI y los procedimientos de relaciones con las terceras partes	Revisión de actividades con proveedores mediante el catálogo electrónico del portal de Compras Públicas	Se establece una planificación por parte del establecimiento y por medio del portal del Sistema de contratación pública se realiza las Compras por catálogo para cada contrato con terceros, el responsable del contrato es manejado por el estado y el responsable del proyecto es quien informa al Rectorado el avance del mismo
No esta seguro			DS2.3 - Administración de riesgos del proveedor	No se aplica					Entrevista con el Jefe del Centro de Informática	No existe documentación	No administran riesgos del proveedor esa actividad gestiona el estado
No esta seguro			DS2.4 - Monitoreo del desempeño del proveedor	No se aplica					Entrevista con el Jefe del Centro de Informática	No existe documentación	No existe un proceso para el monitoreo de prestación del servicio esa actividad gestiona el estado

3.3.6.2 Evaluación de los controles para el proceso DS7 Educar y Capacitar a los Usuarios

En la tabla 3.11 se muestran los resultados de la evaluación de los controles para el Proceso DS7.

Tabla 3. 11 Evaluación de los controles para el Proceso DS7

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			DS7 Educar y capacitar a los usuarios	Pobre					Entrevista con el Jefe del Centro de Informática	Oficio de Aprobación del Rector	El proceso de programa de capacitación se lo realiza en base a oficios aprobados por el Rector
No Documentado			DS7.1 - Identificación de necesidades de entrenamiento y educación	Pobre					Pedido de programa de entrenamiento	No existe documentación	Los usuarios tienen capacitación de los portales, pero no tienen conocimiento de los manuales de usuario y no se lleva un programa de entrenamiento
Documentado			DS7.2 - Impartición de entrenamiento y educación	Muy Bueno					Encuesta a los usuarios	Oficio de Aprobación	Los usuarios tienen capacitación cuando son solicitados individualmente o por medio de oficio
No Documentado			DS7.3 - Evaluación del entrenamiento recibido	Pobre					Entrevista al personal del Centro de Informática	No existe documentación	No se realiza una evaluación al entrenamiento impartido

3.3.6.3 Evaluación de los controles para el proceso DS10 Administrar los Problemas

En la tabla 3.12 se muestran los resultados de la evaluación de los controles para el Proceso DS10.

Tabla 3. 12 Evaluación de los controles para el Proceso DS10

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
Documentado			DS10 Administrar los problemas	Pobre					Entrevista al personal del Centro de Informática	Procedimiento de custodia de equipos informáticos y para el seguimiento se lleva un registro de los oficios autorizados por el Rector	Existe un proceso de manejo de problemas que asegura que todos los eventos operacionales sean analizados y resueltos de manera oportuna pero no se generan reportes de incidentes para problemas significativos
	No Documentado		DS10.1 - Identificación y clasificación de problemas	Pobre					Entrevista al Jefe del Centro de Informática	No existe documentación	Tienen establecido nivel 1 y nivel 2 para clasificar los incidentes a nivel de Help Desk
Documentado			DS10.2 - Rastreo y resolución de problemas	Pobre					Entrevista al Jefe del Centro de Informática	No se tiene un Sistema de gestión de problemas, para el seguimiento se lleva un registro de los oficios autorizados por el Rector	Se tiene definido procedimientos para el manejo de problemas, cuando se tiene un problema se reporta al Centro de Informática y se atiende todos los problemas vía telefónica o por oficio pero no se tiene un proceso interno de TI que permita gestionar de manera eficiente las incidencias

Tabla 3. 12 Evaluación de los controles para el Proceso DS10 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
No Documentado			DS10.3 - Cierre de problemas	Pobre					Pedido de procedimientos para el cierre de incidentes	No se documenta	Todos los problemas reportados se solucionan a tiempo no se sigue un procedimiento particular para el cierre de incidencias
Documentado			DS10.4 - Integración de las administraciones de cambios, configuración y problemas	Muy Bueno					Pedido de procedimientos para el manejo de problemas	Procedimiento de custodia de equipos informáticos. Fichas de Equipo	Existe procedimiento para asegurar la integración entre los cambios, la disponibilidad, el sistema y el personal de manejo de la configuración

3.3.7 Procesos del Dominio de Monitorear y Evaluar

3.3.7.1 Evaluación de los controles para el proceso ME1 Monitorear y Evaluar el Desempeño de TI

En la tabla 3.13 se muestran los resultados de la evaluación de los controles para el Proceso ME1.

Tabla 3. 13 Evaluación de los controles para el Proceso ME1

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
			MONITOREAR Y EVALUAR								
Documentado			ME1 Monitorear y evaluar el desempeño de TI				Pobre		Entrevista al Jefe del Centro de Informática	Indicadores de evaluación de la gestión en el área informática del Instructivo para el funcionamiento de los Centros de Informática (CDI) y Secciones Informáticas (SEI) del Ejército Ecuatoriano	No se tiene una efectiva administración de desempeño, el proceso de monitoreo lo hacen en base al instructivo pero no es puesto en práctica al 100 por ciento
No esta seguro			ME1.1 - Enfoque del Monitoreo				No se aplica		Entrevista con el Jefe del Centro de Informática	No existe documentación	No hay planes de monitoreo
Documentado			ME1.2 - Definición y recolección de datos de monitoreo		Muy Bueno				Evaluación de los procesos de tecnología y de control interno	Indicadores de evaluación de la gestión en el área informática del Instructivo para el funcionamiento de los Centros de Informática (CDI) y Secciones Informáticas (SEI) del Ejército Ecuatoriano	Se tienen indicadores y parámetros de la medida del funcionamiento de los procesos tanto internos como teóricos de igual manera monitorea y optimiza el funcionamiento y rendimiento de las base de datos
No Documentado			ME1.3 - Método de monitoreo				Pobre		Entrevista con el Jefe del Centro de Informática	No existen documentos de método de monitoreo	Tienen implantado un método en el proceso de monitoreo pero no hay un documento del proceso que sea oficial

Tabla 3. 13 Evaluación de los controles para el Proceso ME1 (Continuación)

CONTROL INTERNO			PROCESOS DE IT	DESEMPEÑO					EVALUACIÓN		
Documentado	No documentado	No esta seguro		Excelente	Muy Bueno	Satisfactorio	Pobre	No se aplica	Pruebas Realizadas	Documento de Respaldo	Resultados
No Documentado			ME1.4 - Evaluación del desempeño	Muy Bueno					Verificación de datos de reportes de monitoreo de desempeño de procesos	No existe documentación	Los servicios son medidos por el Jede del Centro de Informática al optimizar el funcionamiento de la base de datos y por el Administrador de hardware en el momento que están monitoreando los pedidos de ayuda. Esto es un servicio continuo
Documentado			ME1.5 - Reportes al Consejo Directivo y a Ejecutivos	Muy Bueno					Revisión de informes de monitoreo, funcionamiento y reportes	Histórico de respaldos realizados copias de informes y oficios	Cuando se entregan servicios implementados se realiza una calificación de lo que se recibe a esto se suma las copias de informes y oficios que son su respaldo
Documentado			ME1.6 - Acciones Correctivas	Pobre					Entrevista con el Jefe del Centro de Informática	Instructivo para el funcionamiento de los Centros de Informática (CDI) y Secciones Informáticas (SEI) del Ejército Ecuatoriano	Revisión de las respuestas de administración en base al instructivo del Comando de Educación y Doctrina del Ejército no es aplicado de manera exhaustiva

3.4 Determinación del Nivel de Madurez

Para hacer que los resultados sean utilizables con facilidad en resúmenes gerenciales se determinará el nivel de madurez de los procesos de control de cada uno de los dominios definidos por COBIT como se muestra en la Figura 3.2:

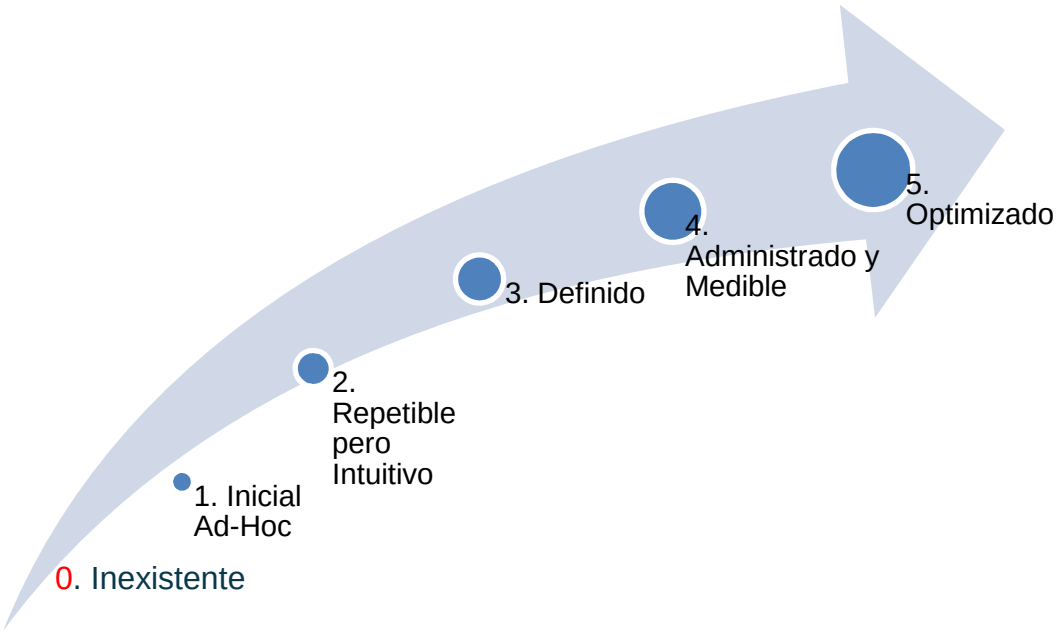


Figura 3. 2 Niveles de Madurez

0 – No se aplican procesos administrativos en lo absoluto.
1 – Los procesos son ad –hoc y desorganizados
2 – Los procesos siguen un patrón regular
3 – Los procesos se documentan y se comunican
4 – Los procesos se monitorean y se miden
5 – Las buenas prácticas se siguen y se automatizan

3.4.1 Nivel de Madurez del Dominio de Planificación y Organización

A continuación se muestra en la Figura 3.3 el Nivel de Madurez en el que se encuentra el Centro de Informática de la Institución para el dominio PO.

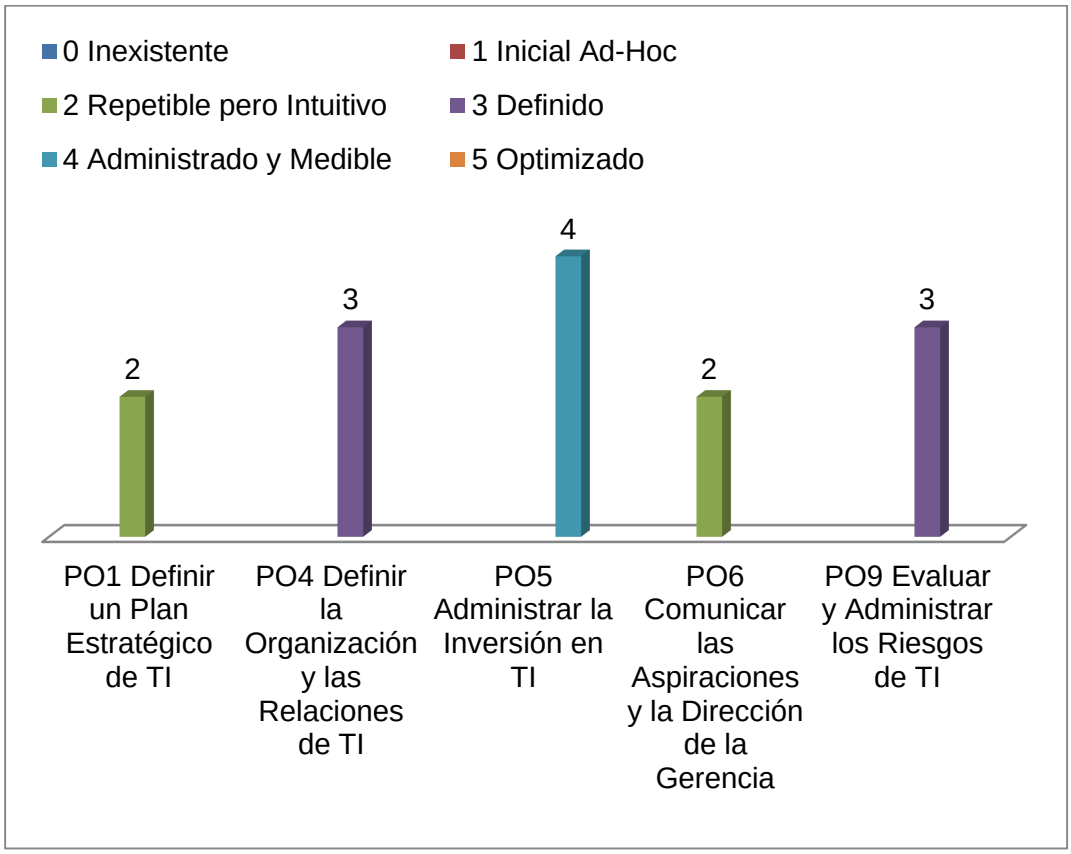


Figura 3. 3 Nivel de Madurez del Dominio de Planificación y Organización

3.4.1.1 Proceso PO1: Definir un Plan Estratégico de TI

Nivel de Madurez Determinado: Repetible pero Intuitivo

Las políticas definidas en el establecimiento al seguir lineamientos de entidades militares siguen un enfoque estructurado, el cual se documenta y se da a conocer a todo el personal informático.

La planeación estratégica de TI de la Institución es poco razonable debido a que la actualización de estos planes de TI ocurre como respuesta solamente cuando se ha solicitado por parte de la Dirección en este caso del Rectorado y se discute en reuniones la orientación del negocio que tiene el Departamento Informático. Sin embargo no existen procedimientos para analizar el proceso de manera ágil porque insisten en un direccionamiento oficial que deben seguir pero no lo realizan completamente.

3.4.1.2 Proceso PO4: Definir la Organización y las Relaciones de TI

Nivel de Madurez Determinado: Definido

Existe un entendimiento implícito de las necesidades para una organización de TI en el Departamento Informático, los roles y responsabilidades están formalizadas y fortalecidas.

La organización de TI está desarrollada para responder tácticamente a las necesidades del usuario y se encuentra funcionalmente completa.

Se tiene definida las funciones a ser realizadas por parte del personal de TI pero no las que deben realizar los usuarios. Los requerimientos esenciales de personal de TI y experiencia están definidos y satisfechos.

3.4.1.3 Proceso PO5: Administrar la Inversión en TI

Nivel de Madurez Determinado: Administrado y Medible

La responsabilidad y la rendición de cuentas por la selección y presupuestos de inversiones se asignan adecuadamente. Al ser una Institución pública debe seguir procedimientos y políticas establecidas por el Estado las cuales exigen que se ejecuten identificando y resolviendo las diferencias existentes en el presupuesto.

Los procedimientos gubernamentales exigen además realizar un análisis formal de costos que cubran los costos directos e indirectos de las operaciones existentes, como las propuestas de inversiones considerando todos los costos a lo largo del ciclo de vida.

Se utiliza un proceso de presupuesto estándar el mismo que debe ser realizado detalladamente para ejecutar los planes de inversiones anuales. Por último los beneficios y los retornos se calculan en términos financieros y no financieros todo esto en base a las políticas implantadas por parte del estado.

3.4.1.4 Proceso PO6: Comunicar las Aspiraciones y la Dirección de la Gerencia

Nivel de Madurez Determinado: Repetible pero Intuitivo

La administración tiene un entendimiento implícito de las necesidades y requerimientos de un ambiente efectivo de control de información. Sin embargo las prácticas no están consistentemente documentadas.

La administración ha comunicado la necesidad de control, políticas y procedimientos estándar, pero el desarrollo se ha dejado a discreción de los administradores individuales y de las áreas de negocio. Las políticas para soportar documentación son desarrolladas en base a necesidades individuales y no hay un marco de referencia global.

La calidad es reconocida como una filosofía deseable, para ser seguida pero las prácticas se dejan a discreción de los jefes departamentales. El entrenamiento se realiza de forma individual, según se requiera.

3.4.1.5 Proceso PO9: Evaluar y Administrar los Riesgos de TI

Nivel de Madurez Determinado: Definido

Existe un enfoque de evaluación de riesgos desarrollado muy bueno como es el plan de contingencia y el plan de seguridades de la Institución y se implementa a discreción de los jefes departamentales. La administración de riesgos se da por lo general a alto nivel sin embargo no se aplica a proyectos grandes y se aplica solo en fuerza mayor o como respuesta a problemas.

Los procesos de mitigación de riesgos sigue un proceso definido estándar muy bueno y está documentado sin embargo actualmente no se ha realizado una evaluación de riesgos de TI, y los riesgos relativos a TI que afectan las operaciones del día a día son pocas veces discutidas en reuniones de la Dirección.

La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se deja a discreción del personal de la Institución.

3.4.2 Nivel de Madurez del Dominio de Adquisición e Implementación

A continuación se muestra en la Figura 3.4 el Nivel de Madurez en el que se encuentra el Centro de Informática de la Institución para el dominio AI.

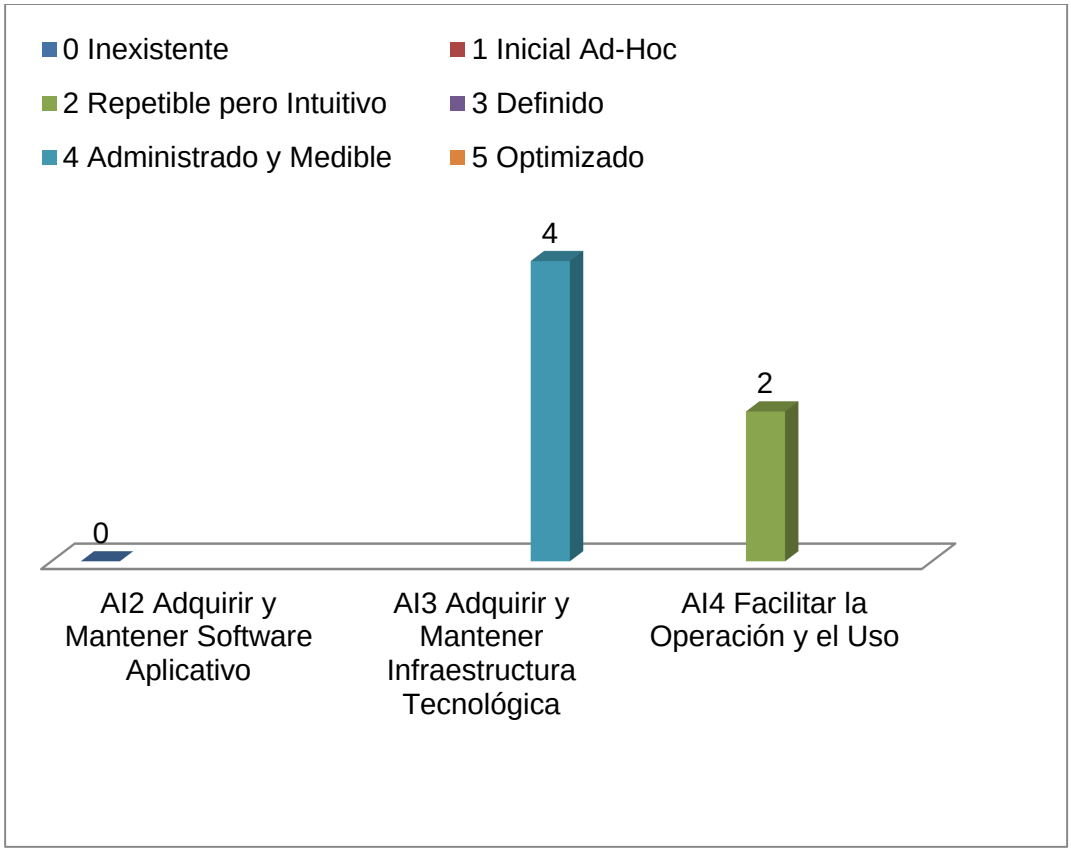


Figura 3. 4 Nivel de Madurez del Dominio de Adquisición e Implementación

3.4.2.1 Proceso AI2: Adquirir y Mantener Software Aplicativo

Nivel de Madurez Determinado: No Existe

No existe un proceso de diseño y especificación de aplicaciones. Casi siempre, las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales.

Es posible que se hayan adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares de la Institución, teniendo como resultado ineficiencias en el mantenimiento y soporte. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación.

3.4.2.2 Proceso AI3: Adquirir y Mantener Infraestructura Tecnológica

Nivel de Madurez Determinado: Administrable y Medible

La adquisición y procesos de mantenimiento de la infraestructura de la tecnología tienen un buen control a tal punto que funciona bien para la mayoría de las situaciones, con un buen seguimiento de las etapas, tanto en lo nuevo como en lo ya existente.

Los procesos son bien organizados a menudo preventivos en el costo en tiempo han sido controlados, aunque no optimizados y todo esto es parte de un plan táctico.

3.4.2.3 Proceso AI4: Facilitar la Operación y el Uso

Nivel de Madurez Determinado: Repetible pero Intuitivo

Se utilizan enfoques similares para generar procedimientos y documentación, pero no se basan en un enfoque estructural y no tienen un marco de trabajo.

No hay un enfoque uniforme para el desarrollo de procedimientos del usuario y de operación. El Departamento Informático genera los materiales de entrenamiento y la calidad depende del personal informático que se involucra.

Los procedimientos y la calidad del soporte al usuario van desde pobre a muy buena con una consistencia e integración muy pequeña a lo largo de la organización. Se proporcionan o facilitan programas de entrenamiento para el negocio y los usuarios, pero no hay un plan general para ofrecer o dar entrenamiento.

3.4.3 Nivel de Madurez del Dominio de Entrega y Soporte

A continuación se muestra en la Figura 3.5 el Nivel de Madurez en el que se encuentra el Centro de Informática de la Institución para el dominio DS.

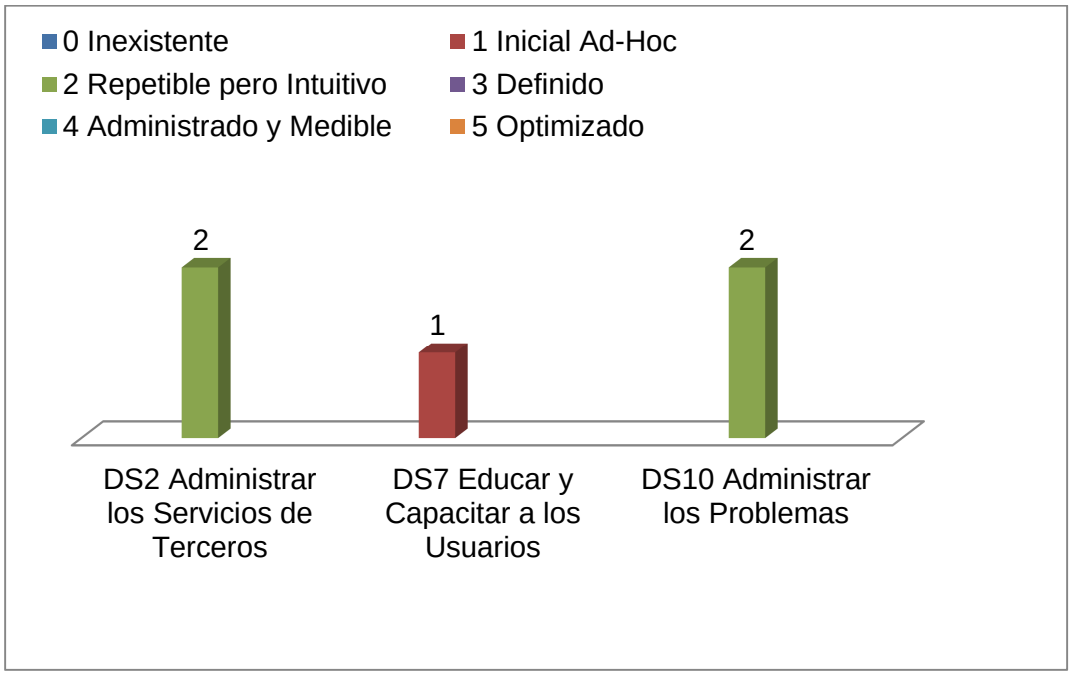


Figura 3. 5 Nivel de Madurez del Dominio de Entrega y Soporte

3.4.3.1 Proceso DS2: Administrar los Servicios de Terceros

Nivel de Madurez Determinado: Repetible pero Intuitivo

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

3.4.3.2 Proceso DS7: Educar y Capacitar a los Usuarios

Nivel de Madurez Determinado: Inicial / Ad Hoc

Hay evidencia de que la organización ha reconocido la necesidad de contar con un programa de entrenamiento y educación, pero no hay procedimientos estandarizados. A falta de un proceso organizado, los empleados han buscado y asistido a cursos de entrenamiento solicitando al Departamento Informático.

El enfoque global de la dirección carece de cohesión y solo hay comunicación esporádica e inconsistente respecto a los problemas y enfoques para hacerse cargo del entrenamiento y la educación.

3.4.3.3 Proceso DS10: Administrar los Problemas

Nivel de Madurez Determinado: Repetible pero Intuitivo

Se ha calificado con este valor porque hay una amplia conciencia sobre la necesidad y los beneficios de administrar los problemas relacionados con TI, tanto dentro de las áreas de negocio como en la función de servicios de información. El proceso de resolución ha evolucionado un punto en el que el personal informático clave son responsables de identificar y resolver los problemas. La información se comparte entre el personal de manera informal y reactiva. El nivel de servicio hacia la comunidad usuaria varía y es obstaculizado por la falta de conocimiento estructurado a disposición del administrador de problemas.

3.4.4 Nivel de Madurez del Dominio de Monitorear y Evaluar

A continuación se muestra en la Figura 3.6 el Nivel de Madurez en el que se encuentra el Centro de Informática de la Institución para el dominio ME.

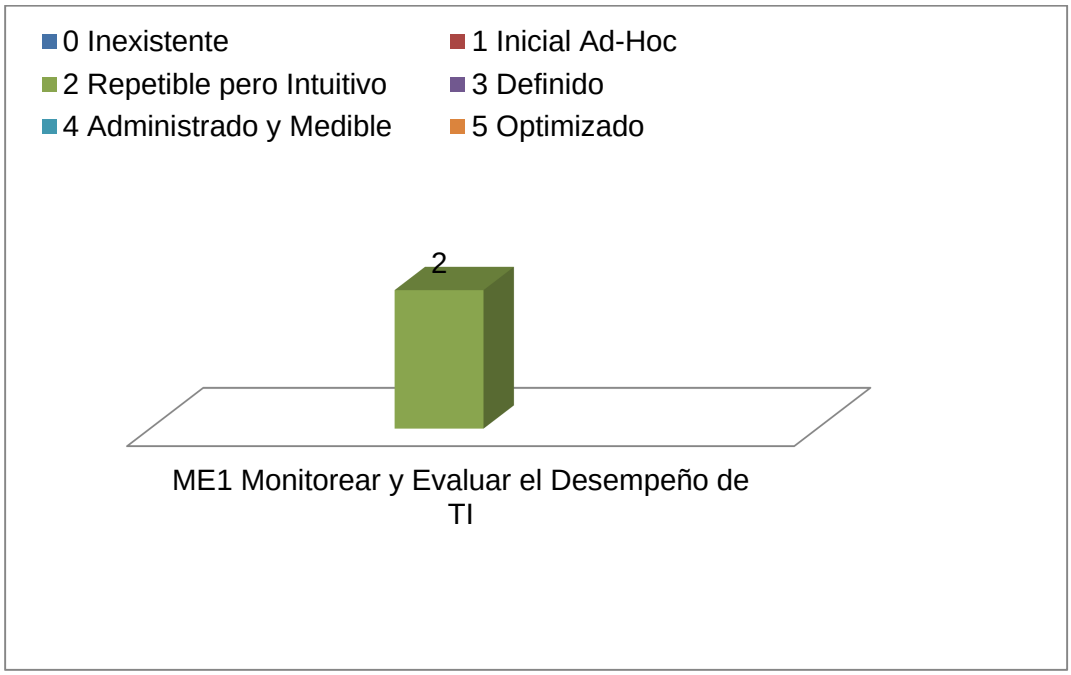


Figura 3. 6 Nivel de Madurez del Dominio de Monitorear y Evaluar

3.4.4.1 Proceso ME1: Monitorear y Evaluar el Desempeño de TI

Nivel de Madurez Determinado: Repetible pero Intuitivo

Se han identificado algunas mediciones básicas a ser monitoreadas sin embargo el Departamento Informático no lleva a cabo monitoreo de proyectos o procesos de forma independiente, no se cuenta con reportes útiles oportunos y precisos.

Los métodos y las técnicas de recolección y evaluación existen pero los procesos no se han adoptado en toda la organización. La interpretación de los

resultados del monitoreo se basa en la experiencia del personal informático clave.

Herramientas limitadas son seleccionadas y se implantan para recolectar información, pero esta recolección no se basa en un enfoque planeado.

CAPÍTULO 4

INFORME FINAL DE LA AUDITORÍA

4.1 Informe Ejecutivo

4.1.1 Introducción

Son muchos los problemas que se presentan al gestionar las Tecnologías de la Información, principalmente en el sentido de cómo lograr que las TI conlleven a una ventaja para la organización, como hacer que las TI sean una inversión con retorno y no solamente un gasto necesario. Para eliminar estos inconvenientes se han creado diversos marcos de trabajo y mejores prácticas como es COBIT (Control Objectives for Information and related Technology) en español Objetivos de control para la información y tecnologías relacionadas, para realizar una gestión de TI adecuadamente.

Este modelo de referencia ayuda a evaluar la planeación, estructuración, dirección y control de la función informática dentro de la Institución del Colegio Militar Nº 10 “Abdón Calderón”, permitiendo realizar un informe final que proporciona las recomendaciones realizadas por el Auditor tomando en cuenta las observaciones que se han generado durante todo el proceso de la Evaluación.

Posteriormente de realizar la revisión de la documentación del COMIL Nº 10 y ejecutar el análisis de acuerdo a la guía de Auditoría del estándar de COBIT, el documento del informe final además incluye un resumen gerencial y un grupo de conclusiones y recomendaciones obtenidos al realizar la revisión

de cada uno de los procesos para ayudar a la toma de decisiones en la Institución.

Este documento es para uso restringido y solo será utilizado bajo la autorización de la Dirección del Centro de Informática del COMIL Nº 10.

4.1.2 Resumen Ejecutivo

4.1.2.1 Antecedentes

El proyecto de Evaluación Técnica Informática del Colegio Militar Nº 10 Abdón Calderón fue comprendido en un estudio detallista de la realidad actual de la tecnología de información de la Institución y de las posibles recomendaciones para la implantación de controles y mejoramiento de TI; el mismo que fue aprobado por el Señor Rector de la Institución y planificado en el Centro de Informática del Colegio y ejecutado a través del Departamento de Ciencias de la Computación como proyecto de tesis de grado.

El objetivo principal de la Auditoría, es detectar si la gestión del Departamento de TI del COMIL Nº 10 es competente para cubrir todas las necesidades de la Institución en materia de desarrollo, mantenimiento, atención al usuario, equipamiento, conectividad, manejo de proyectos, seguridades y planificaciones, validando que los proyectos de TI aporten con la consecución de los objetivos de la Institución, efectiva y eficientemente.

La Auditoría se planificó tomando como modelo COBIT, planteado por un organismo internacional de estandarización como es ISACA, a fin de identificar

debilidades y emitir recomendaciones que permitan mitigar los riesgos de la Institución.

El proyecto va dirigido a todos los funcionarios del COMIL Nº 10 que tengan relación con los recursos de tecnología de información como: hardware, software, comunicaciones e infraestructura, teniendo en consideración que la información es un activo invaluable, que debe ser controlado en el caso del Colegio por el Centro de Informática, que le permita cubrir las necesidades de los diversos usuarios del COMIL Nº 10 y no centrarse mayoritariamente en adquisiciones de TI.

4.1.2.2 Descripción Metodológica

El proyecto de la Evaluación Técnica Informática del Colegio Militar Nº 10 Abdón Calderón fue realizado sobre los cuatro dominios del modelo COBIT, Planificación y Organización, Adquisición e Implantación, Entrega y Soporte, Monitoreo y Evaluación; estos procesos fueron ejecutados por un estudiante como proyecto de tesis de grado, y orientados por el Director del proyecto Ing. Mario Ron y La Codirectora Ing. Lourdes De la Cruz.

El desarrollo de la Evaluación Técnica Informática del COMIL Nº 10 cubrirá aspectos de planificación, organización, ejecución de proyectos, seguridades, equipos, redes, comunicaciones e infraestructura, con el objeto de determinar los riesgos a los que se encuentra sometida la Institución y recomendar procedimientos que permitan minimizar o eliminar riesgos.

El trabajo consistió en la aplicación del estándar COBIT, para la Auditoría del Departamento Informático de la Institución, profundizando conocimientos

de un modelo de gobierno de TI y control interno. Realizando la investigación de los procesos que se consideran prioritarios para la Institución, considerando su funcionamiento e importancia, además evaluando los posibles riesgos según los eventos que hayan afectado al proceso.

Los siguientes procesos y objetivos de control de TI agrupados en cuatro dominios fueron ejecutados en la evaluación:

Planificación y Organización

- PO1 Definir un Plan Estratégico de TI: los criterios de la planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del COMIL Nº 10.
- PO4 Definir la Organización y las Relaciones de TI: el Centro de Informática de la Institución se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión; con procesos, políticas de gestión y procedimientos para todas las funciones.
- PO5 Administrar la Inversión en TI: establecer un marco de trabajo para administrar los programas de inversión en Tecnologías de Información que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal y medible.
- PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia: criterios de dirección en base a un marco de trabajo de control empresarial para TI, definiendo y comunicando las políticas.

- PO9 Evaluar y Administrar los Riesgos de TI: crear y dar mantenimiento a un marco de trabajo de administración de riesgos; el marco de trabajo documenta un nivel común y estrategias de mitigación y riesgos de TI.

Adquisición e Implementación

- AI2 Adquirir y Mantener Software Aplicativo: criterios de información que se aplican irán enmarcados sobre parámetros de efectividad, eficiencia, integridad, cumplimiento y confiabilidad, llegando a proporcionar funciones automatizadas que soporten efectivamente los procesos del negocio y la especificación de los requerimientos funcionales y operacionales.
- AI3 Adquirir y Mantener Infraestructura Tecnológica: criterios de información de efectividad, eficiencia e integridad, proveyendo al proceso de las plataformas apropiadas a las aplicaciones del negocio. La forma de lograrlo se dirige a una adquisición apropiada de hardware y software, estandarización de software, y un consistente sistema de administración.
- AI4 Facilitar la Operación y el Uso: el conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI de todos los procesos que ejecuta el Centro de Informática, y proporciona entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la infraestructura y así entregar al usuario final la información integra y en el tiempo justo.

Entrega y Soporte

- DS2 Administrar los Servicios de Terceros: este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos.
- DS7 Educar y Capacitar a los Usuarios: se requiere identificar las necesidades de entrenamiento de cada grupo de usuarios, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo que incremente la productividad y mida los resultados.
- DS10 Administrar los Problemas: el proceso requiere la identificación y clasificación de problemas, la verificación y confirmación de soluciones adecuadas, en base al propósito deseado y criterios de información, efectividad, integridad y disponibilidad con la realización de un plan formalizado de gestión de problemas.

Monitorear y Evaluar

- ME1 Monitorear y Evaluar el Desempeño de TI: se requiere un proceso de monitoreo, incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos y tomar medidas expeditas cuando existan desviaciones para garantizar que se hagan las cosas correctas y que estén de acuerdo con el conjunto de direcciones y políticas.

Dentro del análisis de los Objetivos de Control para la aplicación del estándar COBIT se considera la visión objetiva e independiente, punto de vista

crítico y sistemático, basado en evidencias, bajo normas y metodologías aprobadas a nivel internacional como COSO, ITIL, ISO: 17799, 27001; que ayudaron en la selección de muestras de las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados, llegando a obtener una opinión profesional e imparcial enfocada en aspectos a nivel de la gestión de las Tecnologías de Información, criterios de información y prácticas de controles requeridos para determinar la eficiencia en el uso de los recursos informáticos, validez de la información y efectividad de los controles establecidos.

A más de la aplicación del modelo COBIT se realizaron entrevistas al personal y se utilizaron herramientas de implementación para la recolección de la información como:

- Entrevistas con las personas de las áreas del Departamento Informático; Administración de: Base de Datos y Software, Hardware, Redes y Telecomunicaciones del Centro de Informática del COMIL Nº 10.
- Reuniones con el Rector del COMIL Nº 10.
- Reuniones constantes con el Jefe del Centro de Informática del COMIL Nº 10.
- Investigación documental de los procedimientos, actividades, proyectos, registros, instructivos, pruebas, informes, memorandos, contratos. Del manejo de hardware, software, comunicaciones, infraestructura y recursos humanos de la Institución.

Después de la fase de recolección de información, se procedió al análisis que incluye la elaboración de las matrices de riesgos y de investigación de campo que incluye los 4 dominios del modelo por cada objetivo que se ha seleccionado con un estudio y análisis minucioso, en este caso se evaluó 12 objetivos de alto nivel con sus respectivos sub-objetivos que llegan al número 72, posteriormente se categoriza el modelo de madurez para cada objetivo de alto nivel, que permiten tener una medición del estado actual de los procesos administrativos y de tecnología de información definidos, y la capacidad que estos tienen en el cumplimiento de las actividades diarias en el COMIL Nº 10.

Finalmente las observaciones encontradas pasan a formar parte del análisis de presentación de resultados, donde las autoridades del COMIL Nº 10 y los involucrados directos con tecnologías de información recibirán el Informe de Auditoría con las observaciones, criterios, condiciones, causas y efectos hallados en el análisis, además las recomendaciones respectivas para la aplicación en la Institución.

4.1.2.3 Principales Hallazgos

Durante la evaluación se pudo realizar ciertos ajustes en base a las últimas actividades desarrolladas por el Departamento Informático, y a las justificaciones presentadas, obteniendo una serie de resultados los mismos que resumimos en las siguientes afirmaciones:

1. No se tiene un esquema para evaluar si los proyectos de TI cumplen con los objetivos institucionales. Por lo que se recomienda establecer un comité estratégico del Departamento de TI para la gestión de

proyectos de TI que involucre a las direcciones principales de la Institución, y que sean quienes definan en conjunto la tendencia y prioridades en la ejecución de proyectos.

2. La metodología empleada actualmente para la gestión de TI en la Institución, depende del Instructivo para el funcionamiento de los Centros de Informática (CDI) y Secciones Informáticas (SEI) por parte del Ejército Ecuatoriano el cual esta diseñado para administrar las unidades militares a nivel Informático de manera estándar y con normas por parte del estado como es la Senplades para la gestión de proyectos. Se recomienda por lo tanto que la Institución adopte un proceso que gestione de buena manera el desarrollo de proyectos de TI y que se realice evaluaciones de los mismos para desempeñar las normativas administrativas eficientemente.
3. No existen políticas de aseguramiento de niveles de servicio, de calidad, de monitoreo, para los procesos de tecnología de información, por lo que se sugiere llevar a cabo un seguimiento continuo del desarrollo de los procesos, usando modelos como los de COBIT o un estándar para la gestión de servicios como ITIL, y realizando evaluaciones permanentes, siendo aconsejable hacerlas como mínimo cada seis meses.
4. No se tiene una difusión amplia de las metodologías para evaluar y administrar los riesgos de TI dentro del personal del Departamento Informático del COMIL Nº 10, por lo que la identificación de riesgos y la calidad de respuestas no son las mejores pese a que se tienen planes de seguridad y contingencia satisfactorios. De modo que se

debe involucrar a las personas del Departamento Informático, en el proceso de transmitir las metodologías de análisis de riesgos que se definan en cualquier proyecto de TI.

Después de la conclusión de todo el análisis y evaluación de la realidad actual de la Tecnología de información del COMIL Nº 10, se han detectado falencias importantes que se detallan a continuación.

El modelo de madurez del Dominio Planificación y Organización muestra para cada objetivo lo siguiente:

- Para definir un plan estratégico el COMIL Nº 10 alcanza un nivel de madurez repetible pero intuitivo, existen políticas definidas en el establecimiento que siguen normas militares estructuradas sin un enfoque metodológico, la planeación estratégica de TI de la Institución es insuficiente debido a que la actualización de estos planes de TI ocurre como respuesta cuando se ha solicitado por parte de la Dirección y no existen procedimientos para analizar el proceso de manera ágil y realizarlo completamente.
- Para la definición de la organización y las relaciones de TI en el Centro de Informática alcanza un nivel de madurez determinado definido, los roles y responsabilidades están formalizadas y se encuentra funcionalmente completa, se tiene definida las funciones a ser realizadas por parte del personal de TI pero no las que deben realizar los usuarios, los requerimientos esenciales del personal de TI y experiencia están definidos, pero el entendimiento de las

necesidades no se fortalecen para la organización de TI en el Departamento Informático.

- Para la administración de la inversión en TI del COMIL Nº 10 el nivel de madurez es administrado y medible, se utiliza un proceso de presupuesto estándar el mismo que debe ser realizado detalladamente para ejecutar los planes de inversiones anuales, la responsabilidad y la rendición de cuentas por la selección y presupuestos de inversiones se asignan adecuadamente, al ser una Institución pública debe seguir procedimientos y políticas establecidas por el estado las cuales se ejecutan identificando y resolviendo las diferencias existentes en el presupuesto, exigen además realizar un análisis formal de costos que cubran los costos directos e indirectos de las operaciones existentes, como las propuestas de inversiones.
- Para comunicar las aspiraciones y la dirección de la Gerencia obtiene un nivel de madurez repetible pero intuitivo, la administración ha comunicado la necesidad de control, políticas y procedimientos estándar, pero la comprensión y la utilización por parte de toda la Institución no ha sido factible, el desarrollo se ha dejado a discreción de los administradores individuales, jefes departamentales y de las áreas de negocio, las políticas para soportar documentación no son desarrolladas en base a necesidades individuales y no hay un marco de referencia global.
- Para evaluar y administrar los riesgos de TI de la Institución alcanza un nivel de madurez definido, existe un enfoque de mantenimiento y evaluación de riesgos con un plan de contingencia y plan de

seguridades de la Institución, implementado a discreción de los jefes departamentales, la administración de riesgos se da por lo general a buen nivel sin embargo no se evalúan los costos y no se aplica a proyectos grandes y casi siempre se aplica solo en fuerza mayor o como respuesta a problemas.

El modelo de madurez del Dominio Adquisición e Implementación muestra para cada objetivo lo siguiente:

- Para adquirir y mantener software aplicativo adquiere un nivel de madurez no existente, debido a que no se tiene un proceso de diseño y especificación de aplicaciones, no se siguió ninguna metodología para evaluarlo y adquirirlo. Las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales, se han adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares de la Institución, teniendo como resultado deficiencias en el mantenimiento y soporte del software aplicativo.
- Para adquirir y mantener infraestructura tecnológica alcanza un nivel de madurez administrable y medible, la adquisición y procesos de mantenimiento de la infraestructura de tecnología tiene un buen control a tal punto que funciona bien para la mayoría de las situaciones, con un buen seguimiento de las etapas, tanto en lo nuevo como en lo ya existente, los procesos son bien organizados a

menudo preventivos en el costo en tiempo han sido controlados, aunque no optimizados y todo esto es parte de un plan táctico.

- Para facilitar la operación y el uso el nivel de madurez es repetible pero intuitivo, se utilizan enfoques similares para generar procedimientos y documentación, pero no se basan en un enfoque estructural y no tienen un marco de trabajo, no hay un enfoque uniforme para el desarrollo de procedimientos de usuario y de operación, el Departamento Informático genera los materiales de entrenamiento y la calidad depende del personal informático que se involucra.

El modelo de madurez del Dominio Entrega y Soporte muestra para cada objetivo lo siguiente:

- Para administrar los servicios de terceros adquiere un nivel de madurez repetible pero intuitivo, el proceso de supervisión de los proveedores de servicios de terceros, de los riesgos asociados y de la prestación de servicios es informal. Se utiliza un control pro-forma con términos y condiciones estándares del proveedor (por ejemplo, la descripción de servicios que se prestarán). Los reportes sobre los servicios existen, pero no apoyan los objetivos del negocio, la responsabilidad de administrar los proveedores y la calidad de los servicios prestados está asignada, actualmente este proceso lo maneja el estado, sin embargo se asigna la responsabilidad de planificación y gestión de proyectos por parte del Centro de Informática monitoreando el cumplimiento de las condiciones operativas, de control y se implantan acciones correctivas, la

Dirección Informática ajusta el proceso de adquisición y monitoreo de servicios de terceros.

- Para educar y capacitar a los usuarios obtiene un nivel de madurez inicial, hay evidencia de que la organización ha reconocido la necesidad de contar con un programa de entrenamiento y educación, pero no hay procedimientos estandarizados, a falta de un proceso organizado, los empleados han buscado y asistido a cursos de entrenamiento solicitando al Departamento Informático, solo hay comunicación esporádica e inconsistente respecto a los problemas y enfoques para hacerse cargo del entrenamiento y la capacitación.
- Para administrar los problemas el nivel de madurez es repetible pero intuitivo, hay una amplia conciencia sobre la necesidad y los beneficios de administrar los problemas relacionados con TI, tanto dentro de las áreas de negocio como en la función de servicios de información, el proceso de resolución ha evolucionado un punto en el que el personal informático clave son responsables de asegurar que todos los eventos operacionales sean analizados y resueltos de manera oportuna sin embargo no se generan reportes de incidentes para problemas significativos y es obstaculizado por la falta de conocimiento estructurado a disposición del administrador de problemas.

El modelo de madurez del Dominio Monitorear y Evaluar muestra para cada objetivo lo siguiente:

- Para monitorear y evaluar el desempeño de TI la Institución alcanza un nivel de madurez repetible pero intuitivo, se han identificado

algunas mediciones básicas a ser monitoreadas sin embargo el Departamento Informático no lleva a cabo monitoreo de proyectos o procesos de forma independiente, no se cuenta con reportes útiles oportunos y precisos, los métodos y las técnicas de recolección y evaluación existen pero los procesos no se han adoptado en toda la organización, herramientas limitadas son seleccionadas y se implantan para recolectar información, pero esta recolección no se basa en un enfoque planeado.

La implementación de COBIT es una necesidad básica de cualquier tipo de organización que busca en reforzar sus actividades y encontrar en los recursos de TI el sustento para el éxito de todas sus transacciones. COBIT se define como un modelo para la dirección del negocio que sirve para la investigación, desarrollo, publicación y promoción de un marco de trabajo de control sobre la definición adecuada de los procesos de tecnología de información.

La adquisición de COBIT es una prioridad en el COMIL Nº 10, para prevalecer los procesos de tecnología de información y su relación con los objetivos del negocio.

El desarrollo del modelo de COBIT presenta facilidad de comprensión y entendimiento, pero depende del criterio de cada auditor la aplicación que se proporcione.

4.2 Informe Detallado

4.2.1 Auditoría Informática del Colegio Militar Nº 10 Abdón Calderón

En conformidad con el Plan del proyecto de tesis, “Evaluación Técnica Informática del Colegio Militar Nº 10 Abdón Calderón”, se ha determinado las áreas y procesos más importantes, para focalizar en las áreas de mayor riesgo realizando la revisión de los controles referentes a los cuatro dominios que soporta COBIT la Planeación y Organización, Adquisición e Implementación, Entrega y Soporte y Monitorear y Evaluar implantados en Tecnología de la Información y Comunicaciones del COMIL Nº 10, se ha evaluado el estado actual del Departamento Informático, para establecer las recomendaciones orientadas a mejorar el nivel de gestión del Departamento de TI.

La metodología empleada ha sido recopilación de información mediante entrevistas, cuestionarios, estudio documental de información entregada por el establecimiento, información que fue tabulada y detallada en matrices de control, antes ya expuesta en el Capítulo 3 del presente trabajo. Este documento pretende ser una herramienta útil para la Dirección de TI, como una guía para el mejoramiento del servicio prestado por el Departamento Informático.

El proyecto fue conformado por el auditor John Alexis Narváez Mejía.

A continuación se detallan las observaciones y recomendaciones resultantes de la revisión, en base al estándar COBIT.

PO1. DEFINIR UN PLAN ESTRATÉGICO DE TECNOLOGÍA DE INFORMACIÓN

PO1.1 Administración del Valor de Tecnología de Información

Observación PO1: El Centro de Informática no elaboró de manera adecuada el plan estratégico de tecnología de información.

Criterio –

"Trabajar con el negocio para garantizar que el portafolio de inversiones de TI de la empresa contenga programas con casos de negocio sólidos. Los procesos de TI deben proporcionar una entrega efectiva y eficiente de los componentes TI de los programas y advertencias oportunas sobre las desviaciones del plan, incluyendo costo, cronograma o funcionalidad, que pudieran impactar los resultados esperados de los programas. La rendición de cuentas del logro de los beneficios y del control de los costos es claramente asignada y monitoreada. Establecer una evaluación de los casos de negocio que sea justa, transparente, repetible y comparable, incluyendo el valor financiero, el riesgo de no cumplir con una capacidad y el riesgo de no materializar los beneficios esperados".

Condición –

- El COMIL Nº 10 posee un Plan Estratégico Informático, en el cual existe evidencia que no se ha seguido un marco de trabajo y participación activa del Centro de Informática (Evidencia: Plan Estratégico de Organización 2008-2009).

- Existen documentos de planeación y normas institucionales que no son elaborados por el Departamento Informático, el cumplimiento de estos se los realiza en base a las políticas del Comando de Educación y Doctrina del Ejército y de la Senplades. (Evidencia: Instructivos y Normas del Comando de Educación y Doctrina del Ejército Ecuatoriano para el Centro de Informática (CDI) y Secciones Informáticas (SEI), Normas y Formatos de la Secretaría Nacional de Planificación y Desarrollo (Senplades)).
- El COMIL Nº 10 tiene un plan informático anual de trabajo, elaborado por el Centro de Informática de la Institución en base al presupuesto operativo anual, sin embargo no refleja un control de costos y no existe evaluaciones para los requerimientos o necesidades emergentes de la Institución (Evidencia: Lineamientos y Políticas de Planificación y Ejecución de la Programación Anual de la Política Pública 2012-2013).

Causa –

- La falta de un marco de trabajo y participación activa del Departamento de Tecnología de Información, no permite dirigir estratégicamente las metas de la Institución.
- No se aplican metodologías, instructivos o normas relacionadas a gobierno de Tecnología de Información.
- Dentro de la Institución se cumplen las políticas por imposición y no por convicción propia, sin enfocarse a estrategias efectivas de dirección y control que salvaguarden los intereses de la Institución.

Efecto –

- Si no existe una Planificación Estratégica Informática, con la participación activa del Departamento de Tecnología de la Información, no se puede obtener estrategias de negocio que puedan ser competitivas, arriesgando el patrimonio de la Institución.
- La falta de metodologías, estándares, normas y procedimientos definidos institucionalmente para la planificación estratégica, implica el desarrollo de objetivos incorrectos, metas inalcanzables y planes con bajo desempeño.
- La ejecución incorrecta de políticas institucionales origina una desviación en el enfoque de los objetivos.

Recomendación PO1:

- El Jefe del Centro de Informática, deberá realizar hasta el segundo trimestre del año lectivo 2012-2013, la evaluación del Plan Estratégico Informático, para una actualización del mismo, luego del análisis y diseño de una metodología o proceso acorde con la Institución; como por ejemplo la “Metodología activa de integración o de planificación en paralelo”; integrando las posibilidades de TI y la participación activa del personal del Departamento Informático.
- El Jefe del Centro de Informática, utilizará un marco de trabajo, estándares, normas y procedimientos relacionados a gobierno de Tecnología de Información que fortalezca la administración de TI, con el análisis organizacional en base a perspectivas y metas a alcanzar durante el año, en alineación con la Planificación

Estratégica Institucional y la Planificación Estratégica de Tecnologías de Información.

- El Jefe del Centro de Informática, establecerá un marco metodológico para desarrollar políticas de tecnologías de información, que incluya la clasificación, identificación y evaluación de los riesgos en materia de tecnología, así como su administración y documentación.

PO1.2 Alineación de Tecnología de Información con el negocio

Observación PO2: Las estrategias de la Institución no están relacionadas con las estrategias de Tecnologías de Información.

Criterio –

"Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades. Las estrategias de negocio y de TI deben estar integradas, relacionando de manera clara las metas de la Institución y las metas de TI y reconociendo las oportunidades así como las limitaciones en la capacidad actual, y se deben comunicar de manera amplia".

Condición –

- En base a la investigación de campo, las estrategias de la Institución no están integradas con las estrategias de Tecnologías de información (Evidencia: Plan Estratégico Institucional).

- Las proyecciones de la Institución, no se encuentran alineadas a las necesidades y requerimientos del Departamento Informático del COMIL Nº 10. (Evidencia: Plan Estratégico Institucional).

Causa –

- No existe evidencia de que las estrategias de la Institución estén vinculadas con el plan estratégico informático.
- Falta de conocimiento por parte del personal del COMIL Nº 10 y del personal del Centro de Informática, acerca de la Planificación estratégica y su importancia, no hay comunicación de manera amplia de las metas institucionales y de las metas de TI.

Efecto –

- La falta de lineamientos de metas estratégicas del establecimiento, con las metas estratégicas de Tecnologías de Información, no permite tener una base objetiva del negocio, para mejorar el desempeño de TI.
- No es posible desarrollar el plan estratégico de manera correcta, al no tener personal capacitado en temas de planificación estratégica organizacional.

Recomendación PO2:

- El Jefe del Centro de Informática durante los dos primeros trimestres del año lectivo, procederá a incluir estrategias de Tecnologías de información dentro de las estrategias institucionales, para establecer

prioridades acordadas en la participación del Departamento Informático y en el mejoramiento del Plan Estratégico Institucional.

- El Jefe del Centro de Informática durante el año lectivo 2012-2013, organizará y ejecutará un plan de capacitación acerca de la Planificación Estratégica de Tecnologías de Información, a todo el personal informático de la Institución.

PO1.3 Evaluación del Desempeño y la Capacidad Actual

Observación PO3: No se realiza una evaluación de desempeño de los planes existentes de TI.

Criterio –

"Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades".

Condición –

- Los documentos de planificación que el Centro de Informática utiliza, no son evaluados, ni monitoreados para su mejora, simplemente se apoyan en instructivos implementados por entidades militares y aplicados de manera intuitiva (Evidencia: Instructivos y Normas del Comando de Educación y Doctrina del Ejército Ecuatoriano: Centro de Informática (CDI) y Secciones Informáticas (SEI)).

- No existe evidencia de planes de los sistemas de información (Evidencia: No existe documentación).

Causa –

- Falta de calidad en los instructivos facilitados por las entidades militares.
- Falta de políticas de evaluación y monitoreo de los planes de TI.
- No existe adaptación de las características, las definiciones, los objetivos, los métodos y los sistemas de los instructivos, con la organización y funcionalidad de la Institución.

Efecto –

- Utilizar instructivos que no se basan en un marco de trabajo y que solamente sirven de guía para orientar a la Institución de la función tecnológica debido a que su capacidad esta centrada de manera general, ocasiona inconvenientes en la Dirección de TI, especialmente en el seguimiento y control de los sistemas de información, y de la estructura tecnológica.
- La falta de una metodología, estándares y procedimientos formales en la administración de TI, proporciona al proceso de planeación establecer un esquema sin prioridades en los objetivos del negocio y no se cuantifique cuáles de los requerimientos del negocio son posibles, poniendo en riesgo la asignación de recursos de TI.

Recomendación PO3:

- Durante los dos primeros trimestres del año lectivo, el Jefe del Centro de Informática deberá evaluar los planes existentes fundamentándose en un marco de trabajo de mejores prácticas como COBIT y en normas técnicas de control interno a nivel de gestión de TI.
- El Jefe del Centro de Informática establecerá dentro del año lectivo 2012-2013, las políticas necesarias para definir metodologías, estándares y procedimientos en el proceso de análisis de factibilidad para proyectos inmersos en la planificación de TI, incluyendo políticas de ejecución de seguimiento y evaluación.

PO1.4 Plan Estratégico de TI

Observación PO4: El plan estratégico Informático no está estructurado, ni elaborado de acuerdo a los objetivos estratégicos de la Institución.

Criterio –

"Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos. El plan estratégico de TI define cómo se cumplirán y medirán los objetivos, debe incluir el presupuesto de la inversión operativo, las fuentes de financiamiento, la estrategia de obtención, la estrategia de

adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI".

Condición –

- El documento de planeación del Departamento Informático no cumple los requisitos y criterios de evaluación exigidos por COBIT, debido a que no existen procedimientos detallados en el plan, como: políticas, normas y presupuestos para delinear el trabajo.

Causa –

- Falta de dirección Estratégica y Planificación de TI contemplada en el diseño organizacional. (Evidencia: Plan Informático de Organización 2008-2009).
- No existe evidencia de un proceso para adaptar los cambios al plan estratégico informático a largo plazo en la Institución, y no hay políticas de desarrollo y mantenimiento de Planes (Evidencia: Plan Informático de Organización 2008-2009).

Efecto –

- La falta de dirección estratégica y planificación de TI en el Departamento Informático, conduce a desarrollos informáticos que no dan respuesta oportuna ni confiable a las necesidades de información requerida por los usuarios de la Institución.

- La falta de un enfoque estructurado al proceso de planeación a largo plazo, no permite tener como resultado un plan de alta calidad que cumpla los objetivos institucionales.

Recomendación PO4:

- El Jefe del Centro de Informática durante el año lectivo 2012-2013 deberá evaluar y actualizar el plan estratégico de TI para cumplir y medir los objetivos, debe tener el detalle suficiente para permitir la definición de planes de proyectos, como los costos y riesgos relacionados.
- El Jefe del Centro de Informática establecerá y aplicará un enfoque estructurado al proceso de planeación a largo y corto plazo de TI, para conseguir un plan de alta calidad, considerando la revisión anual e incluyendo el presupuesto de inversión, y ajustando el Plan Estratégico de Informática cuando se considere necesario.

PO1.5 Planes Tácticos de TI

Observación PO5: Se tiene errores en la estructura, contenidos y procedimientos en los planes que se manejan actualmente.

Criterio –

"Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI, estos planes tácticos deben describir las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados.

Los planes tácticos deben tener el detalle suficiente para permitir la definición de planes de proyectos. Administrar de forma activa los planes tácticos y las iniciativas de TI establecidas por medio del análisis de los portafolios de proyectos y servicios".

Condición –

- La planificación que el Centro de Informática ejecuta es únicamente a corto plazo y limitada por el presupuesto asignado anualmente en función del gasto de cada período. (Evidencia: Plan anual de Trabajo).
- No se administra de forma continua los planes informáticos y no se lleva de manera ágil los procedimientos recomendados por las entidades a las que son sujetos (Evidencia: Plan anual de Trabajo, Plan de mantenimiento de hardware, Plan de Seguridad de la Información).

Causa –

- La Planificación inadecuada de TI y desinformación del personal encargado del Departamento Informático.
- Falta de políticas de gestión continua organizacional.

Efecto –

- La falta de planificación de tecnologías de información en el Centro de Informática, produce desvíos en el rumbo estratégico a largo plazo y es probable que no se pueda controlar los eventos

importantes en términos de pérdida de tiempo, riesgo de gastos que dejan de estar al alcance de la Institución.

- La falta de políticas de control, evaluación y seguimiento de la Función de TI, no permite el mejoramiento de los servicios y la toma de decisiones.

Recomendación PO5:

- El Jefe del Centro de Informática durante el año lectivo 2012-2013 deberá implementar un portafolio de planes tácticos de TI, los mismos que deben derivar del plan estratégico de TI, además deben describir las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos serán administrados.
- Durante cada año lectivo el Jefe del Centro de Informática realizará una planificación de TI apropiada y constante, actualizará los planes existentes, utilizando procedimientos como guías para mejorar.
- El Jefe del Centro de Informática, implementará políticas de control estableciendo los lineamientos y disposiciones de responsabilidades para evaluar y monitorear la planificación de TI (semestralmente).

PO4. DEFINIR LA ORGANIZACIÓN Y LAS RELACIONES DE TI

PO4.1 Marco de Trabajo de procesos de TI

Observación PO6: No se establece un marco de referencia de control interno de TI en los procesos del Departamento Informático.

Criterio –

"Definir un marco de trabajo para el proceso de TI para ejecutar el plan estratégico de TI. Este marco incluye estructura y relaciones de procesos de TI (administrando brechas y superposiciones de procesos), propiedad, medición del desempeño, mejoras, cumplimiento, metas de calidad y planes para alcanzarlas. Proporciona integración entre los procesos que son específicos para TI, administración del portafolio de la empresa, procesos de negocio y procesos de cambio del negocio. El marco de trabajo de procesos de TI debe estar integrado en un sistema de administración de calidad y en un marco de trabajo de control interno".

Condición –

- Se tiene establecido un marco de referencia de Normas de la Senplades para cumplir los objetivos y adecuar las metas a las circunstancias de cambio, sin embargo no se utiliza un marco de trabajo de TI, este proceso aun no se formaliza en el Departamento Informático (Evidencia: No existe evidencia).

Causa –

- Falta de capacitación referida a mejores prácticas y marcos de trabajo de TI por parte del personal del Centro de Informática.

Efecto –

- La falta de comprensión de marcos de trabajo de TI produce deficiencia de análisis y determinación de expectativas no claras y poco realistas de la gestión del Departamento Informático.

Recomendación PO6:

- El Jefe del Centro de Informática en el lapso de tres meses deberá precisar un marco de referencia de control para modelar los procesos, hecho que puede darse utilizando COBIT, ITIL, o cualquier otro conjunto de mejores prácticas.

PO4.2 Comité Estratégico de TI

Observación PO7: No se tiene un comité de gestión de TI en el Centro de Informática.

Criterio –

“Establecer un comité estratégico de TI a nivel de consejo. Este comité deberá asegurar que el gobierno de TI, se maneje de forma adecuada, asesore sobre la dirección estratégica y revise las inversiones principales a nombre del consejo”.

Condición –

- Solamente se tiene una persona encargada del monitoreo de tareas desarrolladas en el Departamento Informático (Jefe del Centro de Informática) (Evidencia: No existe documentación).

Causa –

- Falta de un plan estratégico Informático, en el cual se enmarque las estrategias para el control de la función de TI.

Efecto –

- La falta de un comité estratégico de TI, impide mantener una visión coherente entre los objetivos institucionales y la gestión tecnológica, que determine las falencias con respecto a la evaluación, valoración y actualización tecnológica.

Recomendación PO7:

- El Jefe del Centro de Informática durante el primer trimestre del año lectivo deberá formalizar la creación del comité de TI, en el nivel de Dirección, definiendo sus responsabilidades en base a los procedimientos de gerencia, dirección y vigilancia de TI, guiándose en ITIL (Librería de las mejoras prácticas destinadas a facilitar la entrega de Servicios de TI) para la toma de decisiones importantes y para garantizar que se cumplan los objetivos que plantea la Institución.

PO4.3 Comité Directivo de TI

Observación PO8: El nivel de comunicación entre TI y la Dirección se da a través de reuniones periódicas sin registrar avances en los proyectos.

Criterio –

"Establecer un comité directivo de TI compuesto por la dirección ejecutiva, del negocio y de TI para determinar las prioridades de los programas de inversión de TI alineadas con la estrategia y prioridades de negocio de la empresa, dar seguimiento al estatus de los proyectos y resolver los conflictos de recursos. Monitorear los niveles de servicio y las mejoras del servicio".

Condición –

- No existe un comité de planeamiento que supervise la función de TI y sus actividades. La resolución de artículos de acción a nivel institucional lo realiza el Comité Directivo de la Institución que esta formada por los Jefes Departamentales (Evidencia: No existe documentación).

Causa –

- El Centro de Informática, no posee un proceso definido para la revisión de logros institucionales dentro del área de TI.

Efecto –

- La falta de un Comité Directivo de TI, implica que no se realice seguimiento a los proyectos efectuados en la Institución,

desconociendo su factibilidad para llevar a cabo los objetivos a tiempo y con los resultados necesarios en concordancia con lo establecido.

Recomendación PO8:

- Durante el primer trimestre el Jefe de Investigación y Evaluación junto al Jefe del Centro de Informática desarrollará un Comité Directivo de TI que supervise el progreso de los proyectos con el propósito de verificar tareas y responsabilidades definidas y comunicadas.

PO4.5 Estructura Organizacional

Observación PO9: La estructura organizacional del Centro de Informática no esta definida en todos los niveles de servicios que provee la Institución.

Criterio –

“Establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además implementar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos de negocio esperados y las circunstancias cambiantes”.

Condición –

- No se divide la responsabilidad de cada sub-área y no se considera la función de los consultores de TI en la estructura organizativa de TI (Evidencia: Organigrama Funcional).

Causa –

- Falta de gestión estratégica a nivel institucional, no se mantiene una estructura organizacional informática adecuada en el área de TI.

Efecto –

- Al no disponer de una estructura interna en el Departamento de TI, que permita asegurar la independencia a nivel organizacional, no garantiza soluciones de tecnología de información efectiva.

Recomendación PO9:

- El Jefe del Centro de Informática analizará y evaluará la estructura actual del Centro de Informática durante el primer trimestre del año lectivo, deberá dividir la responsabilidad de cada sub-área y considerar la función externa de consultores de TI en la estructura departamental de manera que la dirección estratégica se enfoque en la importancia de las capacidades y rendimiento de la función de TI, que apoye en el mejoramiento de la Institución.

PO4.6 Establecimiento de Roles y Responsabilidades

Observación PO10: No se tiene establecido reglamentos y políticas necesarias para cada miembro del personal del Centro de Informática.

Criterio –

"Definir y comunicar los roles y las responsabilidades para el personal de TI y los usuarios que delimiten la autoridad entre el personal de TI y los usuarios finales y se defina la rendición de cuentas para alcanzar las necesidades del negocio".

Condición –

- No se han dado las directrices (Políticas, Normas y Estándares) para el control de la Función de TI y sus actividades. (Evidencia: Responsabilidades de la Planificación).
- Las funciones generales del Centro de Informática se encuentran definidas en el plan informático, sin embargo en el establecimiento no se ejecutan de la manera prevista y existen funciones y responsabilidades no definidas como por ejemplo: manejo de Seguridades de Información, acceso a sistemas, monitoreo de proyectos (Evidencia: Plan Informático de Organización 2008-2009).

Causa –

- Falta de un plan estratégico informático, en el que se defina las funciones y responsabilidades del personal.
- Los procedimientos e instructivos que utiliza la Institución no están integrados con las funciones del Centro de Informática.

Efecto –

- Al no tener definidas las funciones y responsabilidades de TI en el Departamento Informático, no se puede facilitar un soporte oportuno a los requerimientos de la Institución y una estructura organizacional apropiada.

Recomendación PO10:

- El Jefe del Centro de Informática durante los seis primeros meses del año lectivo 2012-2013, deberá definir la función de TI de cada personal clave del Departamento Informático, evaluando los requerimientos del personal, actualizando continuamente los cambios estructurales y minimizando la dependencia de actividades de un solo individuo.
- Durante el año lectivo el Jefe del Centro de Informática establecerá las responsabilidades, políticas y funciones del manejo de los Sistemas de Información, mediante reglamentos y manuales, enmarcados en ITIL (Librería de las mejoras prácticas destinadas a facilitar la entrega de Servicios de TI).

PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento

Observación PO11: No se tiene determinado un mecanismo de difusión de las políticas de seguridad.

Criterio –

“Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado. Definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento. Establecer responsabilidad sobre la administración del riesgo y la seguridad a nivel de toda la organización para manejar los problemas a nivel de toda la empresa”.

Condición –

- El Centro de Informática, no posee una estructura en base a la cual se establezcan responsabilidades en seguridad lógica y física de los activos de información, existe un responsable de seguridad lógica, pero la seguridad física no tiene un encargado, excepto por la seguridad integral general de la Institución (Evidencia: Plan Informático de Organización 2008-2009).
- No existen Políticas de seguridad de la información. Los esquemas de seguridad están establecidos a nivel de control de acceso y seguridades de información (firewall, antivirus, manejo de claves, etc.). (Evidencia: No existe documentación).

Causa –

- Falta de Dirección de Tecnologías de Información.
- Falta de definición de procesos, funciones y políticas de seguridad de información.

Efecto –

- La inexistencia de políticas que regulen y establezcan la seguridad lógica y física de los activos de información, incrementa el riesgo de acceso ilegal a la información como: acceso de intrusos a las redes y sistemas, fraudes, alteraciones o pérdida de información crítica.

Recomendación PO11:

- El Jefe del Centro de Informática, en el lapso de tres meses establecerá políticas y procedimientos para la correcta administración y asignación formal de la responsabilidad de la seguridad lógica y física de los activos de información del COMIL Nº 10, tomando en cuenta las mejores prácticas para el manejo de los mismos (Estipulados en ITIL).
- El Jefe del Centro de Informática, en el manejo de seguridades de información durante cada año lectivo deberá mantener un historial de todos los controles que se realicen y se debe establecer un mecanismo de difusión y seguimiento de las políticas de seguridad de la información en la Institución.

PO4.9 Propiedad de Datos y de Sistemas

Observación PO12: No existe un esquema de responsabilidad sobre los bienes de la Institución.

Criterio –

“Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información. Los dueños toman decisiones sobre la clasificación de la información y de los sistemas y sobre cómo protegerlos de acuerdo a esta clasificación”.

Condición –

- El Centro de Informática no tiene reglas definidas para el acceso a la información y de sistemas, no hay una definición de custodio o propietario del almacenamiento de la misma y quien sea el responsable de respaldarla (Evidencia: Inventario de Estados Internos con Lista de activos asignados al personal).

Causa –

- Falta de gestión, dirección y control de la Dirección del Centro de Informática para establecer los propietarios de los datos y de sistemas.
- Falta de responsabilidad de supervisión.

Efecto –

- Al no poseer un esquema en el que se establezcan los propietarios y custodios de los datos y sistemas, se consigue manipulación, pérdida, modificación y difusión no autorizada de la información.

Recomendación PO12:

- El Jefe del Centro de Informática en el lapso de tres meses proporcionará procedimientos y herramientas que permitan determinar las responsabilidades de propiedad de datos y de sistemas en la Institución. Además deberá clasificar la información de los bienes y sobre como protegerlos, este proceso debe estar formalizado.

PO4.14 Políticas y Procedimientos para Personal Contratado

Observación PO13: No se tiene definidas e implementadas políticas y procedimientos para los consultores de TI.

Criterio –

"Asegurar que los consultores y el personal contratado que soporta la función de TI cumplan con las políticas organizacionales de protección de los activos de información de la empresa de tal manera que se logren los requerimientos contractuales acordados".

Condición –

- No existe gestión del personal externo contratado en la Institución. (Evidencia: No existe documentación).

Causa –

- Falta de gestión de la Institución para la asignación de consultores y personal contratado.

Efecto –

- Al no establecer evaluaciones de requerimientos de asignación de personal, no permite obtener personal de excelencia que soporte satisfactoriamente la función de TI en la Institución.

Recomendación PO13:

- El Jefe del Centro de Informática asegurará mensualmente que los consultores y el personal contratado que soporta la función de TI, cumplan los intereses y las políticas de protección de los activos de información de la Institución.

PO5. ADMINISTRAR LA INVERSIÓN EN TI

PO5.1 Marco de Trabajo para la Administración Financiera

Observación PO14: Las inversiones de TI no se planean detenidamente de acuerdo a las necesidades de la Institución.

Criterio –

"Establecer y mantener un marco de trabajo financiero para administrar las inversiones y el costo de los activos y servicios de TI a través del portafolio de inversiones habilitadas por TI, casos de negocio y presupuestos de TI".

Condición –

- El presupuesto no se determina de acuerdo a la priorización de necesidades institucionales, sino únicamente de acuerdo a los techos presupuestarios del COMIL Nº 10 y bajo criterios de (Rector, Jefes Departamentales), (Evidencia: Plan de trabajo realizado por el Centro de Informática en base a los lineamientos y políticas de Planificación y Ejecución por parte del estado).

Causa –

- Procedimientos no apropiados en la planificación y priorización de proyectos.

Efecto –

- Al carecer de un plan de infraestructura tecnológica, no se puede argumentar la necesidad y la importancia de la inversión, para que

pueda formar parte del Plan Operativo Anual y que se asigne el presupuesto necesario.

- Al realizar priorizaciones de los proyectos sin una base técnica, se estaría permitiendo proyectos que no aporten al logro de los objetivos institucionales.

Recomendación PO14:

- El Jefe Financiero desarrollará un mecanismo durante cada año lectivo para que se midan los beneficios y los retornos de la inversión de TI en términos financieros y no financieros para abordar de manera acertada la inversión de TI.
- El Jefe del Centro de Informática establecerá un procedimiento para permitir la presentación de los proyectos con un justificativo y análisis de costos, además de una selección apropiada de alternativas a la solución del problema presentado, para que esto sirva de priorización de los proyectos para el cumplimiento de los objetivos institucionales.

PO6. COMUNICAR LAS ASPIRACIONES Y LA DIRECCIÓN DE LA GERENCIA

PO6.3 Administración de Políticas para TI

Observación PO15: La Dirección Informática no ha implementado políticas de TI acordes a las demandas de la Institución.

Criterio –

“Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir su intención, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Su relevancia se debe confirmar y aprobar en forma regular”.

Condición –

- Las políticas de control interno de TI que actualmente maneja el Centro de Informática no se aplican en base a los requerimientos de la Institución. (Evidencia: Lineamientos y políticas de planificación y ejecución de la programación anual de la política pública de la Fuerza Terrestre 2012-2013. Políticas para el funcionamiento de los centros de Informática (CDI) y secciones informáticas (SEI). Políticas de Educación Regular. Políticas de la Secretaría Nacional de Planificación y Desarrollo (Senplades). Políticas de Seguridad de la Información digital para el empleo en el Ejército Ecuatoriano. Instructivo de políticas de Seguridad de la Información digital para el empleo en el Ejército Ecuatoriano).

Causa –

- Desconocimiento del personal informático de promulgar las normativas sobre sistemas de información y comunicación.

Efecto –

- No se puede administrar y controlar de manera eficiente las incidencias de TI sin políticas de administración tecnológica implementadas en la Institución.
- Se incurre en riesgos de seguridad de información, causada por alteraciones, robo o pérdida, que podría atentar la continuidad del negocio.

Recomendación PO15:

- El Jefe del Centro de Informática deberá implementar hasta el segundo trimestre del año lectivo 2012-2013, procesos bien definidos y estandarizados como políticas de Tecnología de Información en el COMIL Nº 10, de modo que cualquier empleado de la Institución, se acoja a dichas normativas.
- El procedimiento de políticas de TI deberá contemplar la implementación, adquisición, supervisión, capacitación, evaluación, operación y el uso de Tecnología para el desarrollo adecuado de la Institución.

PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

PO9.4 Evaluación de Riesgos de TI

Observación PO16: No se ha registrado una evaluación de riesgos de TI en la Institución.

Criterio –

"Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio".

Condición –

- El plan de contingencia contiene un análisis de riesgos enfocado de forma general al COMIL Nº 10, pero no se contempla los activos de TI. (Evidencia: Plan de Contingencias).
- No se ha designado el responsable de la seguridad, no se identifica soluciones para la mitigación de riesgos y vulnerabilidades. (Evidencia: Plan de Seguridad).

Causa –

- Falta de normatividad y capacitación en gestión de riesgos de TI.

Efecto –

- Escasa capacidad de reacción ante eventos imprevistos que inciden en la continuidad del negocio.

- Al no evaluar los riesgos informáticos provoca contratiempos operacionales, procesos inadecuados, situaciones incontrolables y mayores requisitos normativos.

Recomendación PO16:

- El Jefe del Centro de Informática durante los primeros seis meses del año lectivo 2012-2013 deberá implementar una evaluación de los riesgos de TI que impactan al entorno operacional de la Institución apoyándose en los enfoques estandarizados y los planes de contingencia y de seguridad definidos, estos documentos deben estar formalizados en el Departamento Informático.
- El Jefe del Centro de Informática durante el año lectivo establecerá una política general para la evaluación de riesgos que defina el alcance y los límites, la metodología a ser adoptada para las evaluaciones de riesgos, las responsabilidades y las habilidades requeridas.

AI2 ADQUIRIR Y MANTENER SOFTWARE APLICATIVO

PAI2.3 Control y Posibilidad de Auditar las Aplicaciones

Observación AI1: No se sigue una metodología para evaluar y adquirir el software aplicativo.

Criterio –

"Implementar controles de negocio, cuando aplique en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable".

Condición –

- No existe evaluación periódica de las aplicaciones existentes (Evidencia: No existe documentación de auditoría).

Causa –

- Falta de metodologías y normativas en la planificación de proyectos de software.
- Falta de planes de riesgos en la adquisición, implementación, desarrollo y mantenimiento dentro del análisis de las aplicaciones.

Efecto –

- Al no tener una política de evaluación de los sistemas no se puede valorar el nivel de riesgo del funcionamiento de estas aplicaciones, no se puede controlar el acceso a la información, la seguridad, el tiempo de vida y la capacidad de satisfacer las estrategias y requerimientos de la Institución.

Recomendación AI1:

- El Jefe del Centro de Informática deberá ejecutar evaluaciones periódicas de todo el funcionamiento de TI, especialmente de los sistemas de información, para que contribuyan al mejoramiento operacional de la Institución.

AI2.5 Configuración e Implementación de Software Aplicativo Adquirido

Observación AI2: Los sistemas de información de la Institución son generalmente desarrollados por entidades externas (outsourcing).

Criterio –

"Configurar e implementar software de aplicaciones adquiridas para conseguir los objetivos de negocio".

Condición –

- El Sistema Integrado Educativo es un sistema de información que ha caducado, tiene debilidades en el diseño de protocolos utilizados en las redes, políticas de seguridad deficientes e inexistentes, errores de programación, descuido de los fabricantes, mala configuración de los sistemas informáticos, desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática. (Evidencia: No existe documentación de la configuración base para implementar el Sistema Integrado Educativo (SIE)).

Causa –

- Falta de un estudio minucioso en la implementación del software y control activo en el mantenimiento, para que las actualizaciones del software disminuya inconvenientes futuros.

Efecto –

- Al no realizar un estudio en la adquisición y desarrollo de sistemas, se corre el riesgo de que el software no cumpla con todos los requerimientos reales de la Institución.
- Al no realizar un mantenimiento apropiado a los sistemas se obtiene aplicaciones desactualizadas y limitadas en los servicios modulares.

Recomendación AI2:

- El Jefe del Centro de Informática para la nueva adquisición o implementación del sistema de información de la Institución en el lapso de seis meses deberá tener un plan maestro de desarrollo de software, para poder visualizar claramente los objetivos, las prioridades y los tiempos de ejecución. Se debe definir detalladamente los temas de soporte y mantenimiento.

AI2.6 Actualizaciones Importantes en Sistemas Existentes

Observación AI3: No se sigue un proceso para las actualizaciones de los sistemas y de los nuevos requerimientos.

Criterio –

“En caso de cambios importantes a los sistemas existentes que resulten en cambios significativos al diseño actual y funcionalidad, seguir un proceso de desarrollo similar al empleado para el desarrollo de sistemas nuevos”.

Condición –

- El sistema Integrado Educativo: académico, de secretaría y de colecturía fue adquirido desde 2001 y no se han realizado actualizaciones importantes, el portal web de la Institución es el único sistema que tiene actualizaciones pero no se lleva un registro de los cambios. (Evidencia: Lista de aplicaciones y sistemas actuales del Instructivo CDI y SEI).

Causa –

- Falta de una política de actualización de los sistemas de TI por parte del Centro de Informática.
- Desconocimiento en gestión del cambio de software para maximizar el rendimiento de la Institución.

Efecto –

- Al no adoptar una metodología de desarrollo de software y no mantener actualizados los sistemas de información, puede haber puntos de falla, errores en el código de los sistemas o componentes y no permite ampliar las tareas que deben cumplir los sistemas para lograr resultados óptimos.

Recomendación AI3:

- Durante los seis primeros meses del año lectivo 2012-2013 el Jefe del Centro de Informática deberá implementar una política de actualización o algún mecanismo que permita evaluar los sistemas de información para tomar la decisión de cuando se debe actualizar.
- Se debe guardar todas las versiones de los sistemas existentes, realizar una gestión de cambios y definir un diccionario de datos que pueda ser utilizado por los programadores como respaldo de información para el diseño detallado de la aplicación en cada actualización.

AI2.7 Desarrollo de Software Aplicativo

Observación AI4: Actualmente no se utiliza una metodología para el desarrollo de software.

Criterio –

"Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación, los requerimientos de calidad y estándares de aprobación. Asegurar que todos los aspectos legales y contractuales se identifiquen y direccionen para el software aplicativo desarrollado por terceros".

Condición –

- El Centro de Informática no ha seguido una metodología de desarrollo para el ciclo de vida del sistema integrado educativo, no se tiene ninguna configuración participativa de prototipos, ni de las interfaces de las aplicaciones (Evidencia: No existen documentos del ciclo de vida del sistema académico).

Causa –

- No se incluyen procesos y actividades en el desarrollo de los sistemas, desde la definición de requisitos, la adquisición y configuración de los servicios del sistema, hasta la finalización de su uso.

Efecto –

- Sin un proceso bien definido del ciclo de vida del software, el proyecto no logra concluir o terminar sin cumplir los objetivos previstos, con variedad de fallos inaceptables y sin facilitar una estructura eficiente para que proveedores, desarrolladores, personal de mantenimiento, operadores, gestores y técnicos involucrados en el desarrollo de software usen un lenguaje común.

Recomendación AI4:

- El Jefe del Centro de Informática para casos de requerimientos de sistemas nuevos o de sistemas antiguos, en un lapso de seis meses deberá tener una metodología de desarrollo de sistemas como por ejemplo “Programación Extrema (en inglés eXtreme Programming

XP), Proceso Unificado de Rational (en inglés Rational Unified Process o RUP), Feature Driven Development (FDD)", independientemente del proceso a utilizar se debe aplicar un modelo de ciclo de vida, con el afán de controlar adecuadamente los procesos de configuración, definiendo el orden de las tareas o actividades del modelo del ciclo de vida utilizado para el desarrollo.

AI2.8 Aseguramiento de la Calidad del Software

Observación AI5: No se tiene un plan de aseguramiento de calidad de los sistemas de la Institución.

Criterio –

"Desarrollar, implementar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización".

Condición –

- El aseguramiento de calidad de los sistemas de la Institución se siguen algunos procesos de la norma Iso 9000 y 2000 pero no existe evidencia de planes para su cumplimiento (Evidencia: Instructivo para el funcionamiento de los Centros de Informática (CDI) y secciones informáticas (SEI)).

Causa –

- No existe evidencia de un enfoque de Aseguramiento de la calidad debido a que no hay un plan general de calidad del software.

Efecto –

- Al no tener un plan de aseguramiento de calidad del software, no se puede enfocar a que objetivos o procedimientos de calidad se están realizando los controles.

Recomendación AI5:

- El Jefe del Centro de Informática desde los primeros seis meses del año lectivo 2012-2013 deberá implementar el plan de aseguramiento de la calidad del software, además incluirá en el plan generadores de rastros de auditoría, de tal manera que se pueda acudir a éste tipo de información para prever errores críticos.

AI2.9 Administración de los Requerimientos de Aplicaciones

Observación AI6: No se evidencia un análisis de requerimientos para la implementación de los sistemas existentes.

Criterio –

“Seguir el estado de los requerimientos individuales (incluyendo todos los requerimientos rechazados) durante el diseño, desarrollo e implementación y aprobar los cambios a los requerimientos a través de un proceso de gestión de cambios establecido”.

Condición –

- No hay documentos de los requerimientos, se lo aplica sin basarse en pruebas ni especificaciones (Evidencia: No existe documentación).

Causa –

- No tener una adecuada administración y análisis de los requerimientos de software. Falta de evaluación de especificaciones alternativas y a la integración de requerimientos funcionales y no funcionales.

Efecto –

- Al no realizar un correcto análisis de requerimientos del sistema se obtiene inconvenientes para controlar proyectos complejos, se aumenta retrasos y costos, no existe calidad del software y satisfacción del usuario.

Recomendación AI6:

- El Jefe del Centro de Informática, durante los primeros tres meses de la adquisición o implementación del software deberá tener constancia de un análisis de requerimientos de los sistemas para poder tener hitos de control y cronogramas que restrinjan el desarrollo de los mismos.

AI2.10 Mantenimiento de Software Aplicativo

Observación AI7: No se utiliza un plan de mantenimiento de los sistemas que maneja la Institución.

Criterio –

“Desarrollar una estrategia y un plan para el mantenimiento de aplicaciones de software”.

Condición –

- No hay constancia de un plan de mantenimiento para los sistemas, solucionando solamente actualizaciones del sistema web de la Institución a nivel informativo sin registrar cambios. (Evidencia: No existe documentación).
- No se utiliza licencias en todos los software que utiliza la Institución. (Evidencia: No existe documentación).

Causa –

- Falta de planeación, administración y control del mantenimiento del software. No se tiene una revisión periódica de los sistemas para su correcto funcionamiento y no se adaptan los cambios y requerimientos que se presentan en el negocio.

Efecto –

- Sin un plan de mantenimiento de software no se tiene un mejoramiento de los procesos, aumenta el margen de riesgo de

errores y disminuye la capacidad del negocio perdiendo calidad en los procesos.

Recomendación AI7:

- El Jefe del Centro de Informática durante los primeros seis meses del año lectivo deberá formalizar un plan de mantenimiento para las aplicaciones y sistemas que maneja la Institución que permita involucrar la adaptación y las actualizaciones o cambios de los sistemas.
- El Jefe del Centro de Informática durante el año lectivo 2012-2013 deberá adquirir las licencias de todo el software con los cuales funcionan, para evitar inconvenientes y permanecer dentro de los márgenes de la ley.

AI3 ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA

AI3.1 Plan de Adquisición de Infraestructura Tecnológica

Observación AI8: No se tiene un plan de adquisición de la infraestructura tecnológica en la Institución.

Criterio –

"Generar un plan para adquirir, implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio y que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología".

Condición –

- El único documento que contiene datos sobre la adquisición de infraestructura tecnológica es el plan informático anual realizado por el Centro de Informática pero no contempla la implementación y mantenimiento de la infraestructura tecnológica (Evidencia: Plan Informático Anual).

Causa –

- No hay consistencia entre enfoques tácticos al adquirir y dar mantenimiento a la infraestructura de TI y no existe una programación concisa para el mantenimiento y pruebas de integración con las aplicaciones críticas del negocio.

Efecto –

- Sin una planificación en la adquisición de TI, no hay un control de gastos, no se estandariza los componentes tecnológicos y no se puede tomar acciones frente a eventualidades que afecten la infraestructura tecnológica.

Recomendación AI8:

- En un lapso de seis meses el Jefe del Centro de Informática deberá implementar el plan de infraestructura tecnológica y se deberá considerar extensiones futuras para incrementar capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología.
- El Jefe del Centro de Informática llevará la documentación en cada etapa de ejecución de proyectos de infraestructura tecnológica.

AI3.3 Mantenimiento de la Infraestructura

Observación AI9: No se tiene un plan de mantenimiento de la infraestructura tecnológica.

Criterio –

“Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlen los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión

periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos y requerimientos de seguridad".

Condición –

- El Centro de Informática realiza el mantenimiento de hardware en los centros de cómputo, oficinas de la Institución pero no se sigue un plan específico para el mantenimiento de toda la infraestructura. (Evidencia: Lista de Materiales para Mantenimiento Preventivo y Correctivo. No existe plan de mantenimiento de la infraestructura tecnológica).

Causa –

- Falta de un plan de mantenimiento y programación de la infraestructura tecnológica de la Institución para proteger posibles contratiempos. No llevar acabo un procedente registro del servicio realizado.

Efecto –

- La falta de un plan de mantenimiento a nivel de software y hardware influye en la eficacia y eficiencia de los procesos, existe incremento de incidentes y requerimientos, no se aplica de buena manera el funcionamiento del contingente tecnológico para la integridad de su información, la disponibilidad de sus servicios y la respuesta inmediata a fallos.

Recomendación AI9:

- El Administrador de hardware junto al Jefe del Centro de Informática, durante los seis primeros meses del año lectivo, deberán implementar el plan de mantenimiento de la infraestructura tecnológica y formalizar los procesos de mantenimiento y de soporte de TI, realizar un seguimiento a los registros de las actividades de mantenimiento tecnológico, y mejorar los procesos por medio del uso de herramientas de helpdesk.

AI3.4 Ambiente de Prueba de Factibilidad

Observación AI10: A nivel de hardware y software no se tiene un proceso de pruebas de factibilidad.

Criterio –

"Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo. Hay que considerar la funcionalidad, la configuración de hardware y software, control de versiones, datos y herramientas de prueba y seguridad".

Condición –

- El proceso de factibilidad solamente involucra lo que es hardware pero el análisis no es amplio, a nivel de software no se lo realiza, no

hay evidencia de pruebas de factibilidad (Evidencia: No existe documentación).

Causa –

- No se tiene una programación de pruebas que facilite evaluar adecuadamente los proyectos. Falta de un proceso de protección y disponibilidad de la infraestructura tecnológica y falta de elaboración de proyectos de adquisición y mantenimiento de TI.

Efecto –

- Al no realizar una adecuada programación de pruebas de factibilidad no permite evaluar el nivel de seguridad de la infraestructura tecnológica ni reducir incidentes, los programas de software dejan de funcionar y no garantiza reducir los riesgos de indisponibilidades de servicio, latencias y tiempos de respuesta.

Recomendación AI10:

- En un lapso de seis meses el Jefe del Centro de Informática deberá formalizar el proceso de pruebas para implantar medidas de control interno, seguridad y auditabilidad, a nivel de software y hardware.
- El Jefe del Centro de Informática, en las primeras fases del proceso de adquisición y desarrollo deberá considerar la funcionalidad, la configuración de hardware y software básico, las pruebas de integración y desempeño, migración entre ambientes, control de las versiones, datos y herramientas de prueba y seguridad.

AI4 FACILITAR LA OPERACIÓN Y EL USO

AI4.1 Plan para Soluciones de Operación

Observación AI11: No existe un plan de soluciones de operación en la Institución.

Criterio –

“Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los interesados puedan tomar la responsabilidad oportunamente por la producción de procedimientos de administración, de usuario y operativos, como resultado de la introducción o actualización de sistemas automatizados o de infraestructura”.

Condición –

- No se tiene identificado los niveles de servicio del Centro de Informática. El manual de procesos que utiliza el Departamento Informático no satisface los requerimientos para que el personal del Departamento Informático de soporte de manera efectiva. (Evidencia: Manual de procesos).

Causa –

- Falta de un plan de solución de operación que clarifique los objetivos, recursos y acciones de la Institución.

- Uso indebido de los procedimientos de operación y sistemas de información así como el déficit de los niveles de servicio y políticas de la Institución.
- No se define correctamente los servicios ofrecidos y no se monitorea la calidad de los mismos respecto a los objetivos establecidos en los SLAs.

Efecto –

- Si no existe un plan de soluciones de operación y gestión de niveles de servicio, ocasiona imprecisión en las tareas desarrolladas para enfrentar situaciones esperadas. Se tiene diferentes intereses y puntos de vista y estos a menudo entran en conflicto, el conflicto es la base de la política institucional, convirtiendo a la tecnología en un medio que no aporta valor a los usuarios.

Recomendación AI11:

- El Jefe del Centro de Informática durante los seis primeros meses del año lectivo 2012-2013 implementará y formalizará los niveles de servicio y desarrollará el plan de solución de operación con los procedimientos estándar de operaciones (SOP) para el control de todo el espectro tecnológico.
- El Jefe del Centro de Informática hasta el segundo trimestre del año lectivo establecerá un mecanismo de actualización de la documentación generada en los proyectos y particularmente en lo que concierne a manuales.

AI4.3 Transferencia de Conocimiento a Usuarios Finales

Observación AI12: No existe un procedimiento definido para la capacitación de los usuarios.

Criterio –

"Transferencia de conocimiento y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de aplicación como apoyo a los procesos del negocio. La transferencia de conocimiento incluye el desarrollo de un plan de entrenamiento que aborde el entrenamiento inicial y al continuo, así como el desarrollo de habilidades, materiales de entrenamiento, manuales de usuario, manuales de procedimiento, ayuda en línea, asistencia a usuarios, identificación del usuario clave y evaluación".

Condición –

- No se tiene un plan de entrenamiento para capacitar a usuarios finales el procedimiento de capacitación que cumple el Centro de Informática es en base a solicitudes formales por parte del usuario (Evidencia: No existe documentación).

Causa –

- Falta de políticas para capacitar a los usuarios. No existen programas de entrenamiento ni planes de capacitación.
- No transmitir el conocimiento y las habilidades necesarias a los usuarios clave.

Efecto –

- El usuario final puede tener bajo rendimiento en sus funciones. Uso indebido de las aplicaciones, manipulación y pérdida de la información en la empresa.

Recomendación AI12:

- Durante los seis primeros meses del año lectivo 2012-2013 el Administrador de Hardware junto con el Jefe del Centro de Informática deberán desarrollar un Plan de entrenamiento que comprenda manuales de procedimiento, manuales de usuario, materiales de entrenamiento, ayuda en línea, asistencia a usuarios y evaluación.

AI4.4 Transferencia de Conocimiento al Personal Operativo y Soporte

Observación AI13: No existe evidencia de un programa de entrenamiento y de manuales orientados a la capacitación del personal operativo y de soporte.

Criterio –

"Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoyen y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos. La transferencia del conocimiento debe incluir el entrenamiento inicial y continuo, el desarrollo

de las habilidades, los materiales de entrenamiento, los manuales de operación, los manuales de procedimientos y escenarios de atención al usuario".

Condición –

- El manual de procesos que utilizan en la Institución no satisface los requerimientos para que el personal de soporte técnico y de operaciones apoyen de manera efectiva (Evidencia: Manual de Procesos).
- Actualmente no se lleva una documentación correspondiente a diseños de aplicaciones, código fuente, base de datos, interfaces y manuales de usuarios. (Evidencia: No existe documentación).

Causa –

- No tomar en consideración un Plan de estudios de entrenamiento, campañas de conocimiento y técnicas de conocimiento de procesos de TI.
- No transmitir el conocimiento y las habilidades necesarias al personal de soporte técnico y de operaciones y no ser conscientes de los riesgos y responsabilidades en las que están involucrados.

Efecto –

- No se puede garantizar la satisfacción de los usuarios finales con escasa organización del personal operativo y soporte, sin ofrecimientos de servicios importantes y sin integrar soluciones tecnológicas dentro de los procesos de la Institución.

Recomendación AI13:

- Durante los seis primeros meses del año lectivo 2012-2013 el Administrador de Hardware junto con el Jefe del Centro de Informática deberán considerar un Plan de entrenamiento y técnicas de control en los procesos de TI para el personal operativo y de soporte del COMIL Nº 10.
- El Jefe del Centro de Informática en un lapso de seis meses deberá involucrar en el desarrollo y diseño de todas las aplicaciones de software la documentación respectiva: código fuente, base de datos, interfaces y manuales de usuarios, es necesario tener planes de soluciones de operación y soporte.

DS2 ADMINISTRAR LOS SERVICIOS DE TERCEROS

DS2.1 Identificación de Todas las Relaciones con Proveedores

Observación DS1: No se tiene una documentación formal de las relaciones técnicas con los consultores.

Criterio –

"Identificar todos los servicios de los proveedores y categorizarlos de acuerdo al tipo de proveedor, significado y criticidad. Mantener documentación formal de relaciones técnicas y organizacionales que cubren los roles y responsabilidades, metas, entregables esperados y credenciales de los representantes de estos proveedores".

Condición –

- No se tiene establecido un mecanismo de relación con los proveedores y no existe documentación (Evidencia: No existe documentación).

Causa –

- Las reglas y las responsabilidades de terceras partes no están definidas de forma clara, no se toma en consideración su administración, monitoreo y no se evalúa periódicamente el desempeño del proveedor.

Efecto –

- Al no identificar las relaciones con los proveedores, no se discute los problemas claves y no se informa de los requerimientos de la Institución para buscar soluciones satisfactorias.

Recomendación DS1:

- El Jefe del Centro de Informática, en el lapso de seis meses deberá realizar evaluaciones de riesgo regulares y programáticas de los proveedores que brindan servicios a los procesos de apoyo de la Institución. Mantener acuerdos de cumplimiento con las empresas proveedoras en lo que concierne a mantenimiento y garantía de las aplicaciones, estableciendo los mecanismos de comunicación apropiados.
- Se debe firmar acuerdos de confidencialidad, seguir ciertas normas jurídicas y éticas. Garantizar que los servicios de terceros estén disponibles cuando sean necesarios, que la percepción de la Institución entre proveedores sea positiva, y que se sostenga relaciones a largo plazo que pueden proporcionar a la Institución acceso a servicio personalizado, ofertas especiales y otros servicios que beneficien al colegio.

DS2.2 Gestión de Relaciones con Proveedores

Observación DS2: No se tiene formalizado el proceso de gestión de relaciones con proveedores de TI.

Criterio –

“Formalizar el proceso de gestión de relaciones con proveedores para cada proveedor. Los dueños de las relaciones deben enlazar las cuestiones del cliente y proveedor y asegurar la calidad de las relaciones basadas en la confianza y transparencia”.

Condición –

- No se establece una planificación por parte del Jefe del Centro de Informática para asegurar la gestión de TI con proveedores, ni se realiza un estudio exhaustivo de los proyectos con terceros (Evidencia: Revisión de actividades con proveedores mediante el catálogo electrónico del portal de Compras Públicas).

Causa –

- Falta de diligencia en las relaciones con terceros, tener relaciones a corto plazo con terceras partes buscando constantemente nuevos proveedores puede presentar limitaciones en los servicios prestados.

Efecto –

- No se puede ofrecer un valor estratégico sin una gestión adecuada con las terceras partes, al buscar constantemente nuevos proveedores aumenta los costes considerablemente a nivel de proyectos, y puede haber incumplimientos de los contratos. Se puede tener prestación de servicios sin ofertas y trabajar con

proveedores enojados, dando una mala imagen de una organización.

Recomendación DS2:

- Mantener un estudio constante y actualizado de proyectos de TI con los proveedores por parte del Jefe del Centro de Informática que permitan salvaguardar los intereses de la Institución.
- La Dirección de TI de la Institución debe trabajar con sus proveedores a largo plazo para crear una fuerte relación de trabajo.

DS2.4 Monitoreo del Desempeño del Proveedor

Observación DS3: No existe un proceso definido para el monitoreo de prestación de servicio del proveedor.

Criterio –

"Establecer un proceso para monitorear la prestación de servicio para asegurar que el proveedor cumpla con los requerimientos del negocio actuales y que se adhiera continuamente a los acuerdos del contrato y que el desempeño sea competitivo con proveedores alternativos y las condiciones del mercado".

Condición –

- No existe evidencia de un proceso para el monitoreo de prestación del servicio (Evidencia: No existe documentación).

Causa –

- Falta de administración de riesgos del proveedor, no tener un monitoreo de las relaciones y del rendimiento operacional.
- No efectuar un seguimiento a la prestación del servicio, a los análisis de gastos, a los contratos operativos, a los pedidos y a la gestión de proveedores.

Efecto –

- Las actividades y el desempeño del proveedor no son competitivos, y no permite garantizar un rendimiento óptimo del servicio prestado.
- No se proporciona una información correcta con las personas involucradas en cada proyecto, permitiendo tener proveedores de bajo desempeño.

Recomendación DS3:

- El Jefe del Centro de Informática durante los seis primeros meses del año lectivo deberá establecer y formalizar el proceso de prestación de servicio que permita monitorear el desempeño y nivel de cumplimiento contractual del proveedor.
- Evaluará la potencialidad de los proveedores, con el fin de garantizar las mejores opciones de servicio y que se adapten a la estrategia Institucional para asegurar la competitividad de los precios, bienes o servicios de calidad, tiempos óptimos de entrega, soporte técnico, altos niveles de servicio y resolución de problemas en forma oportuna.

DS7 EDUCAR Y ENTRENAR A LOS USUARIOS

DS7.1 Identificación de Necesidades de Entrenamiento y Educación

Observación DS4: No se tiene establecido un programa de entrenamiento de usuarios.

Criterio –

"Establecer y actualizar de forma regular un programa de entrenamiento para cada grupo objetivo de empleados, que incluya: Estrategias y requerimientos actuales y futuros del negocio. Valores corporativos (valores éticos, cultura de control y seguridad). Implementación de nuevo software e Infraestructura de TI. Habilidades, perfiles de competencias y certificaciones actuales. Métodos de impartición (aula, web), tamaño del grupo objetivo, accesibilidad y tiempo".

Condición –

- No se identifica las necesidades de capacitación y educación, además no se realiza una evaluación al entrenamiento impartido. (Evidencia: No existe documentación)
- Los usuarios de la Institución no tienen conocimiento de los manuales de usuario. (Evidencia: No existe documentación).

Causa –

- No se han implantado programas de entrenamiento. Falta de guías y manuales de usuario.

Efecto –

- Al no identificar las necesidades de entrenamiento de usuarios en la Institución no se puede mejorar, ni tener crecimiento, innovación, cambios, calidad y productividad adoptando el usuario un rol pasivo dentro del COMIL Nº 10 representando una posición desfavorable para el rendimiento de su desempeño.

Recomendación DS4:

- El Administrador de hardware junto al Jefe del Centro de Informática, desde un lapso de seis meses deberán definir y formalizar un programa de entrenamiento en el que se identifique las necesidades de capacitación en forma individual y general, inclusive se debe realizar una evaluación del entrenamiento recibido.
- El usuario deberá involucrarse en este proceso para optar mayores niveles de innovación y creación, todo esto en función del crecimiento Institucional debido a que las necesidades de entrenamiento conforman el grupo de conocimientos, habilidades, aptitudes y destrezas que el usuario no posee, y que deben ser aprendidos con la finalidad de lograr un desempeño de éxito en su cargo.

DS10 ADMINISTRACIÓN DE PROBLEMAS

DS10.1 Identificación y Clasificación de Problemas

Observación DS5: No se tiene un proceso interno de TI que permita gestionar de manera eficiente la resolución de problemas.

Criterio –

“Implementar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes. Se debe determinar la categoría, impacto, urgencia y prioridad de manera apropiada en grupos o dominios relacionados como hardware, software, software de soporte”.

Condición –

- En el Departamento Informático del COMIL Nº 10 no se tiene establecido los niveles para clasificar los incidentes en términos de helpdesk. No se tiene un Sistema de gestión de incidentes (Evidencia: Para el seguimiento de incidencias se lleva un registro de los oficios autorizados por el Rector).

Causa –

- Falta de administración de Incidentes, desconocimiento en el procedimiento clave de detección de problemas, no registrar los detalles del incidente, no tener una clasificación optima, no proveer una solución, no archivar el problema y no finalizarlo.

Efecto –

- Al presentarse algún tipo de situación desconocida en la Institución, se puede tener incidentes que complican las actividades planificadas interrumpiendo un servicio normal, la cual afecta tanto a los usuarios como a la Institución sin restaurar y solucionar lo antes posible.

Recomendación DS5:

- El Jefe del Centro de Informática, en forma inmediata, deberá implementar un proceso interno a nivel de helpdesk que permita manejar correctamente el seguimiento de consultas y requerimientos de usuarios, registrando las resoluciones de problemas mediante una herramienta tecnológica que proporcione un procedimiento de registro y cierre de incidentes adecuadamente.

DS10.4 Integración de las Administraciones de Cambios, Configuración y Problemas

Observación DS6: No existen procedimientos para asegurar la integración de las administraciones de cambios, configuración y problemas.

Criterio –

“Para garantizar una adecuada administración de problemas e incidentes, se debe integrar los procesos relacionados de administración de cambios, configuración y problemas . Monitorear cuánto esfuerzo se aplica en

apagar fuegos, en lugar de permitir mejoras al negocio y en los casos que sean necesarios, mejorar estos procesos para minimizar los problemas".

Condición –

- No se lleva una integración entre los cambios, la disponibilidad, el sistema y el personal de manejo de la configuración. (Evidencia: No existe documentación solamente hay un procedimiento de custodio de equipos informáticos y fichas de registros).

Causa –

- No se integran los procesos de administración de cambio, configuración con procesos de administración de incidentes y problemas para mantener su mesa de servicio enterada de todas las actividades cambiantes antes, durante y después de algún acontecimiento.

Efecto –

- Al no integrar los procesos relacionados de administración de cambios, configuración y problemas, no permite a la mesa de servicio del Centro de Informática atender los requerimientos, no se notifica a los usuarios afectados con tiempo y no se mantiene a los usuarios informados del estatus de solución.

Recomendación DS6:

- El Jefe del Centro de Informática, hasta el tercer trimestre del año lectivo deberá integrar los procesos relacionados a la administración

de cambios, configuración y problemas, implementando un esquema de seguimiento utilizando indicadores clave.

- Para una administración eficaz de la infraestructura de TI es recomendable documentar sus componentes. La administración de la configuración proporciona la base para la toma de decisiones en la administración de cambios, la negociación de contratos de nivel de servicio y la evaluación de capacidad de TI.
- El Jefe del Centro de Informática, semestralmente se deberá ocupar de identificar, controlar y hacer el seguimiento de todas las versiones de hardware, software, documentación y procesos del Departamento Informático para garantizar que sólo se usen componentes autorizados.

ME 1 MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI

ME1.1 Enfoque del Monitoreo

Observación ME1: No existen datos para reportes de monitoreo de todos los procesos en forma automática.

Criterio –

"Establecer un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para medir la solución y la entrega de servicios de TI y Monitorear la contribución de TI al negocio. Se debe integrar el marco de trabajo con el sistema de administración del desempeño corporativo".

Condición –

- No existe evidencia de planes de monitoreo (Evidencia: No existe documentación).

Causa –

- No utilizar un marco de trabajo como COBIT para monitorear las Tecnologías de Información, no realizar un seguimiento al nivel de riesgos, nivel de operación, nivel de reporte y niveles de servicio.
- Falta de un proceso de mesa de servicio.

Efecto –

- Al no aplicar un marco de trabajo para monitorear el desempeño de TI no se responde de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI.

Recomendación ME1:

- El Jefe del Centro de Informática, hasta el segundo trimestre del año lectivo 2012-2013, deberá utilizar un marco de trabajo como COBIT para el monitoreo de la gestión de TI, implementar un proceso de mesa de servicio y de administración de incidentes para definir procedimientos de seguimiento y escalamiento, basados en niveles de servicio que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información para medir la satisfacción del usuario final respecto a la calidad de la mesa de servicio de TI.
- La Dirección de TI deberá implementar un monitoreo de sus reportes de cumplimiento (mensuales), ya que es una forma de calificar al responsable de hacer el control, el jefe del Centro de informática debe estar pendiente de que se cumpla.

ME1.4 Evaluación del Desempeño

Observación ME2: No se tiene definido el proceso de evaluación de desempeño de TI.

Criterio –

“Comparar de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes”.

Condición –

- En el Centro de Informática los servicios no son medidos, no se monitorea el funcionamiento de sistemas, base de datos y proyectos de TI y no se evalúan los pedidos de ayuda. (Evidencia: No existe documentación).

Causa –

- Falta de una visión estratégica de TI por parte del Departamento Informático, falta de apoyo de la Dirección, falta de acuerdo entre el evaluador y el evaluado, y mala utilización de los resultados de la evaluación de desempeño.
- Inexistencia de políticas de evaluación y control del servicio de TI.

Efecto –

- La falta de evaluación y control de TI, ocasiona que no se tenga los resultados necesarios para poder comparar y medir el desempeño de TI, debido a que no se puede determinar si el servicio cumple con las expectativas de la Institución y tampoco si el usuario está satisfecho con el soporte.

Recomendación ME2:

- El Jefe del Centro de Informática, deberá implementar y formalizar un plan de monitoreo semestral en el Departamento Informático y que se adapte al sistema de monitoreo de la Institución para comparar de forma periódica el desempeño contra las metas.

- El Jefe del Centro de Informática establecerá un estilo de dirección participativo del Departamento Informático y evaluará objetivamente el desempeño de TI, con una periodicidad de al menos una vez al año, aunque lo óptimo es que se lo realice semestralmente.

ME1.6 Acciones Correctivas

Observación ME3: No se aplica acciones correctivas para el proceso de monitoreo y evaluación del desempeño.

Criterio –

"Identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes. Esto incluye el seguimiento de todo el monitoreo, de los reportes y de las evaluaciones con: Revisión, negociación y establecimiento de respuestas de administración. Asignación de responsabilidades por la corrección. Rastreo de los resultados de las acciones comprometidas".

Condición –

- No se realiza una revisión de respuestas de administración solamente se aplica el instructivo del Comando de Educación y Doctrina del Ejército que es deficiente (Evidencia: Instructivo para el funcionamiento de los Centros de Informática (CDI) y Secciones Informáticas (SEI) del Ejército Ecuatoriano).

Causa –

- No se realizan análisis de las necesidades actuales de seguridad y monitoreo de forma periódica. No se tienen establecidas técnicas para la recolección de datos de monitoreo.

Efecto –

- Sin un proceso de monitoreo, no se pueden tomar medidas correctivas para mejorar el desempeño de TI en la Institución.

Recomendación ME3:

- El Jefe del Centro de Informática de forma inmediata, identificará e iniciará medidas correctivas basadas en el monitoreo de desempeño de TI, tomando en cuenta las incidencias dependiendo de la gravedad o repetitividad de la misma, resultados de auditoría y revisión de los sistemas para comprobar el correcto desempeño del mismo y la capacidad para conseguir los resultados esperados.
- El Jefe del Centro de Informática, elaborará reportes mensuales para que los altos mandos de la Institución se enteren del estado de cumplimiento de las metas.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- El estándar de COBIT es un conjunto de mejores prácticas y una de las mejores herramientas de gobierno de TI que permite auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización. La utilización de este modelo requiere evaluar y monitorear el control del negocio y la seguridad TI, de esta manera se puede elaborar una auditoría detallada basada en una revisión crítica y analítica de las tareas y actividades tecnológicas que ayuda a comprender el nivel de seguridad y control para proteger los activos de la compañía.

- En el proceso de la auditoría que se realizó se cumplió con todas las expectativas de este proyecto por parte del Centro de Informática del Colegio Militar Nº 10 Abdón Calderón y se observó que al ser una Institución pública y militar, ejecuta políticas y disposiciones militares empleando instructivos, teorías y ejecución de ideas generalizadas pero sin basarse en frameworks de gestión de TI y necesidades reales requeridas por la Institución, existiendo el riesgo de que la calidad de la administración y servicio de TI sea deficiente y no se considere una adecuada planificación por parte del Departamento Informático.

- Se encontró falencias importantes en el Sistema de Información Integrado Educativo del COMIL Nº 10, es un sistema que ha caducado, además no existe documentación, ni manuales de usuario y como efecto se tiene a una persona encargada del mantenimiento del software, administración BD y soporte a usuarios originando que los servicios que brinda el Departamento Informático a la Institución sean postergados y que no se tenga una planificación adecuada con la cual se pueda verificar que se cubran las necesidades informáticas de la Institución.

- COBIT facilita al Ingeniero en Sistemas a tener otra visión mas objetiva y de un nivel más estratégico para planear, organizar, dirigir y controlar la función informática dentro de una organización debido a que cualquier tipo de empresa puede adoptar el estándar de COBIT, como parte de un proceso de reingeniería en aras de reducir los índices de incertidumbre sobre vulnerabilidades y riesgos de los recursos TI y consecuentemente sobre la posibilidad de evaluar el logro de los objetivos del negocio comprometido en procesos tecnológicos.

5.2 Recomendaciones

- Se recomienda al Centro de Informática del Colegio Militar Nº 10 Abdón Calderón inicie un proceso de implementación del estándar de COBIT, debido a que este modelo es producto de un compendio de experiencias y recomendaciones de profesionales expertos de TI a nivel mundial.

- Se recomienda que para un mejor desempeño del Centro de Informática del COMIL Nº 10 se realicen auditorías anualmente en las áreas de administración de: Base de datos, Software, Hardware, Redes y Telecomunicaciones, revisando especialmente el framework de COBIT, las guías de gestión de TI y las necesidades requeridas de la Institución.

- Se sugiere que se tome acciones en la adquisición o implementación del nuevo sistema académico para la Institución y que cumplan las siguientes características propias del Software como son: flexible, específico, actualizable, con la documentación respectiva efectuando estrategias que permitan tener un mayor control en el proyecto, ayudando a los intereses y requerimientos de la Institución, además se debe definir cada una de las funciones, actividades y responsabilidades específicas adecuadamente para cada individuo involucrado en el Departamento Informático para obtener los mejores resultados.

- Para cualquier empresa que quiera iniciar o mantener un proceso de control, lo primordial es la capacitación del personal involucrado, por lo que se recomienda formar un grupo de personas especializadas, las cuales puedan posteriormente transferir sus conocimientos y técnicas recolectadas a toda la organización. Es importante que la solución ofrecida en las organizaciones soporte COBIT, ya que la tecnología tiene un papel indispensable para ayudar a las empresas a alcanzar los objetivos de Gestión.

BIBLIOGRAFÍA

[1.] COBIT 4.1: www.cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf

[2.] Comité Directivo de COBIT y el IT Governance Institute (2000), Directrices de Auditoría, Tercera Edición

[3.] Procedimientos de Auditoría de Sistemas: www.es.scribd.com/doc/26906140/Procedimientos-de-Auditoria-Se-Sistemas

[4.] Auditoría Interna y Externa: www.muziek-film-kunst.blogspot.com/2010/11/121-auditoria-interna-y-externa.html

[5.] Cobit Sistema de Investigación: www.slideshare.net/Jasik/c-o-b-i-t-sistema-de-investigacin.

[6.] Técnicas y Herramientas TI: www.netconsul.com/tecnicas/index.php?ver=cobit

[7.] Auditoría Informática, William P. Leonard.

[8.] Fundação Bradesco, Governança de TI, Fundamentos de COBIT: www.ev.org.br/Cursos/Paginas/Online.aspx

[9.] ITIL, COBIT, CMMI, PMBOK: Como integrar y adoptar los estándares para un buen Gobierno de TI: www.helkyncoello.wordpress.com/2008/12/08/itil-cobit-cmmi-pmbok-como-integrar-y-adoptar-los-estandares-para-un-buen-gobierno-de-ti/

[10.] Procedimientos de Auditoría Informática: www.elregistroycontrol.com.ar/portal/index.php?option=com_content&view=article&id=49:normas-de-auditoria-informatica&catid=9:articulos&Itemid=61

[11.] Control Objective for Information &related Technology: www.es.scribd.com/doc/56501689/32/%C2%BFPara-que-me-sirve-COBIT

[12.] Gestión de Tecnología de Información, Diagnóstico de la Dirección Tecnológica: www.es.scribd.com/doc/57799186/Trabajo-Final-GTI

[13.] Estructura de COBIT: www.es.scribd.com/doc/50648847/18/Estructura-de-COBIT

[14.] Guía para una Metodología de Auditoría Basada en Riesgos: www.cemla.org/old/actividades/2011/2011-09-XIReunionAuditores/2011-09-XIReunionAuditores-05.pdf

[15.] Control Interno y Auditoría Informática: www.tecno-actualidad.blogspot.com/2010/02/control-interno-y-auditoria-informatica.html

[16.] Modelos de control aplicados a la Auditoría Informática: www.es.scribd.com/doc/38284391/MODELOS-DE-CONTROL-DE-AUDITORIA-INFORMATICA

[17.] Enfoques, Estándares y Directrices de la Auditoría: www.auditoria20101.wikispaces.com/file/view/ISO-IEC-IEEE.pdf