ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

UNIDAD DE RELACIONES DE COOPERACIÓN INTERINSTITUCIONAL

DEPARTAMENTO DE POSGRADOS

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

PROMOCIÓN VII A

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TEMA: “EVALUACIÓN TÉCNICA INFORMÁTICA DE LA PLANEACIÓN Y ORGANIZACIÓN DE LA ESPE SEDE PRINCIPAL”

AUTORES:

MARICELA NATALY ACUÑA GUANOLUISA

HILDA VERONICA CIGUENCIA CULQUI

DIRECTOR:

ING. VICTOR MANUEL PÁLIZ OSORIO

SANGOLQUÍ, MAYO DEL 2015

CERTIFICACIÓN

Se certifica que el trabajo titulado "**EVALUACIÓN TÉCNICA INFORMÁTICA DE LA PLANEACIÓN Y ORGANIZACIÓN DE LA ESPE SEDE PRINCIPAL**", fue desarrollado en su totalidad por las Ing(s). Maricela Nataly Acuña Guanoluisa e Hilda Verónica Ciguencia Culqui, investigación que se ha sido dirigida bajo nuestra supervisión, orientando sus conocimientos y competencias para un eficiente desarrollo del tema y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas ESPE.

Sangolquí, Mayo 2015

Ing. Victor Paliz
DIRECTOR DE TESIS

Ing. Fernando Solis
OPONENTE DE TESIS

DECLARACION DE CONFORMIDAD

Nosotras: Ing. Verónica Ciguencia

Ing. Nataly Acuña

DECLARAMOS QUE:

El proyecto de Grado denominado “Evaluación Técnica Informática de la Planeación y Organización de la ESPE Sede Principal”, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Mayo 2015

Ing. Nataly Acuña

Ing. Verónica Ciguencia

AUTORIZACIÓN DE PUBLICACIÓN

Nosotras: Ing. Nataly Acuña

Ing. Verónica Ciguencia

Autorizamos a la Universidad de las Fuerzas Armadas ESPE, la publicación en la biblioteca virtual de la Institución, del trabajo denominado "EVALUACIÓN TÉCNICA INFORMÁTICA DE LA PLANEACIÓN Y ORGANIZACIÓN DE LA ESPE SEDE PRINCIPAL", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y nuestra autoría.

Sangolquí, Mayo 2015

Ing. Nataly Acuña

Ing. Verónica Ciguencia

DEDICATORIA

Con todo mi amor y respeto a mi madre, por ser mi modelo a seguir, por sus sabios consejos, apoyo incondicional y por siempre impulsarme a seguir adelante.

A mi esposo Kleber, por siempre animarme a conseguir nuevos retos en mi vida profesional.

Nataly

A Dios

Por haberme permitido llegar hasta este punto y haberme dado salud, fuerzas y guía para lograr mis objetivos, además de su infinita sabiduría y amor.

A mis Padres

Por haberme apoyado en todo momento, por sus consejos, por la motivación y por su incondicional amor que me ha permitido ser una persona de bien.

Verónica

AGRADECIMIENTO

A Dios, por darme la vida, sabiduría y fuerzas para conseguir las metas propuestas.

A mi madre Elvia y mi tía Gladis, por ser mis guías y apoyarme siempre con su amor y sabios consejos.

Con mucho amor a mi esposo Kleber por su apoyo, paciencia y sacrificio ayudándome a cumplir esta nueva meta.

Nataly

A mis maestros *por* su gran apoyo *y* motivación para la culminación denuestros estudios profesionalesy para la elaboración de esta tesis

A mis padres quienes a lo largo de toda mi vida han apoyado y motivado mi formación académica, creyeron en mí en todo momento y no dudaron de mis habilidades.

Verónica

INDICE DE CONTENIDO

INDICES DE FIGURAS

INDICE DE TABLAS

RESUMEN

En las organizaciones la información es uno de los recursos más importantes y la tecnología tiene un papel importante en el manejo y uso de la misma, el valor agregado que genere la información es lo marca la diferencia entre las organizaciones por lo que importante mantener la calidad de la información, generar valor realizando inversiones acertadas en TI, eficiencia en la tecnología, manejar los riesgos de TI correctamente, mantener los costos de TI óptimos, la información se ha convertido en un recurso crítico en las organizaciones en todos los sectores ya sean estos financieros, productivos, y de servicios. La pérdida de información se ha convertido en un riesgo que las organizaciones en la actualidad lo toman con la seriedad que esto conlleva y por lo tanto están dando énfasis en las medidas correctivas y preventivas necesarias, por esto es necesarios que las organizaciones dispongan de procesos de Auditoria que analicen la organización y su seguridad, de esta manera eliminará o reducirá al máximo la posibilidad de pérdida de información, fallos en equipos de TI, o procesos inadecuados, detectarán a tiempo fraudes, manipulación de información y de esta manera evitarán considerables pérdidas o fracasos.

PALABRAS CLAVES

- COBIT 5
- PLANEACIÓN Y ORGANIZACIÓN
- EVALUACIÓN
- AUDITORIA
- SISTEMAS TECNOLÓGICOS

ABSTRACT

In organizations, information is one of the most important resources and technology has an important role in the management and use of the same, the value added generated by the information is the mark the difference between organizations so important to maintain the quality of the information, generate value investing right in TI, efficiency in technology manage the risk properly, maintain optimal it costs, information has become a resource critical for organizations in all sectors whether these financial, production, and service. The loss of information has become a risk that organizations currently take it seriously that entails and therefore are giving emphasis on corrective and preventive measures necessary for this is necessary to have organizations audit that examined the Organization and its security, in this way will eliminate or will reduce the possibility of loss of information to the maximum , you, or inadequate processes equipment failures, detected time fraud, manipulation of information and thus avoided substantial losses or failures.

CAPÍTULO I

1. INTRODUCCIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

La Universidad de las Fuerzas Armadas ESPE en la fase que se encuentra de cambios a nivel institucional, tiene problemas con el seguimiento, administración, institución, planificación en el área de Informática, debido principalmente al permanente cambio de autoridades y a la falta de herramientas apropiadas en esta área que ayuden a llevar una administración adecuada.

1.2. FORMULACIÓN DEL PROBLEMA

- ¿Cuáles son los procesos del Dominio Alinear, Planificar y Organizar (AP)?
- ¿Qué procesos del Dominio Alinear, Planificar y Organizar (AP) se encuentran implementados en el departamento de TI?
- ¿Qué procesos del Dominio Alinear, Planificar y Organizar (AP) no se encuentran implementados en el área de TI?
- ¿Qué lineamientos se deben aplicar para la implementación de los procesos del Dominio Alinear, Planificar y Organizar?

Para la Evaluación Técnica Informática de la Planeación eInstitución se utilizará el marco de referencia internacional COBIT 5 específicamente para este caso el Dominio de Alineación, Planificación eInstitución (AP); al finalizar la evaluación se emitirá recomendaciones a la Institución ESPE de los riesgos que tiene el Área Informática y los procedimientos adecuados para mitigarlos o eliminarlos.

1.3. JUSTIFICACIÓN DEL PROBLEMA

COBIT 4.1 está disponible a partir de mayo 2007 la nueva de COBIT5 está disponible desde el 2012 introduce 5 procesos nuevos de Gobierno esto ayuda a las empresas a redefinir las prácticas de Gobierno de TI a nivel

ejecutivo, soporta integración con prácticas del gobierno empresarial, se alinea con ISO/IEC 38500.

La versión COBIT 5 clarifica los procesos del nivel de Gestión incorporando los contenidos de COBIT4.1 Val IT y RISK IT en un nuevo modelo de referencia. COBIT5 ayuda a crear un valor óptimo a las empresas, manteniendo el equilibrio entre:

- Uso de los recursos
- Nivel de riesgos
- Beneficios de los servicios

En lo que respecta al Dominio Alinear, Planificar y Organizar, este contribuye para cumplir los objetivos de la institución, ya que este Dominio está relacionado con la estrategia y las tácticas para identificar la forma como la tecnología de la información ayuda al cumplimiento de estos.

1.4. OBJETIVO GENERAL

Realizar una Evaluación Técnica Informática de la Planeación eInstitución de la UTIC de la ESPE y presentar recomendaciones para la mejora de estos procedimientos usando COBIT 5 y las Mejores Prácticas en el Dominio de Alineación, Planificación eInstitución.

1.5. OBJETIVOS ESPECÍFICOS

- Investigar los procesos que forman parte del Dominio Alinear, Planificar y organizar.
- Evaluar los procesos del Dominio que actualmente tenga en el departamento de TI.
- Realizar recomendaciones de los procesos que no se han implementado y dar lineamientos para que sean creados.
- Elaborar el Plan de Investigación de Campo.
- Elaborar el Informe Final de Auditoría con las conclusiones y recomendaciones respectivas de los hallazgos encontrados.

CAPÍTULO II

2. MARCO TEÓRICO Y ESTADO DEL ARTE.

2.1. ANTECEDENTES

La Universidad de las Fuerzas Armadas ESPE cuenta con la Unidad Tecnología de Información y Comunicación UTIC en la que se centraliza la administración y las actividades de Tecnología de Información y Comunicaciones.

La Evaluación Técnica Informática de la Planeación y Organización de la ESPE Sede Principal contribuirá a mejorar la administración y organización de los proyectos del Área Informática.

La Universidad de las Fuerzas Armadas ESPE, se encuentra en un proceso de cambio a nivel institucional; durante este proceso se presentará una nueva estructura organizacional diferente a la actual; con el aporte que se obtendrá al realizar la evaluación se cubrirá estrategias adecuadas en la Área Tecnológica que optimizará los procesos.

2.2. ITIL

ITIL siglas en inglés (Information Technology Infraestructure Library), siglas en español (Biblioteca de Infraestructura de Tecnologías de Información)es un conjunto de procesos que ayudan a las organizaciones a mejorar la calidad y eficiencia de todas las operaciones involucradas en TI tanto como infraestructura, desarrollo y operaciones del área de TI.(ITIL - Gestión de Servicios TI, 2013)

ITIL es reconocido mundialmente como la fundación de las mejores prácticas de la Gestión de Servicio TI la cual tiene un respaldo por un programa de calificación profesional.(ITIL - Gestión de Servicios TI, 2013)

ITIL V3 es la última versión y lo que trata de hacer es consolidar el modelo ciclo de vida del servicio y lo divide ampliando en varios subprocesos hasta convertirlos en procesos más especializados.(ITIL - Gestión de Servicios TI, 2013)

ITIL V3 se basa en 5 libros de consulta basada en las mejores prácticas se detallan:

Estrategia del Servicio

Es la búsqueda de mejorar los servicios actuales de los clientes comparando a proveedores antiguos versus nuevos proveedores de esta manera se puede renovar los contratos o cancelarlos.(ITIL - Gestión de Servicios TI, 2013)

Para cumplir esto tenemos los siguientes procesos:

- Gestión financiera
- Gestión del portafolio
- Gestión de la demanda

Diseño del Servicio

Esto consiste en verificar y analizar todos los factores que se deben considerar como capacitaciones, infraestructura, seguridad, prevención de desastres.(ITIL - Gestión de Servicios TI, 2013)

Para cumplir esto tenemos los siguientes procesos:

- Gestión de catálogo de servicios
- Gestión de niveles de servicios
- Gestión de la disponibilidad
- Gestión de la capacidad
- Gestión de la Continuidad del Servicio de TI
- Gestión de Proveedores
- Gestión de la Seguridad de Información
- Coordinación del Diseño

Transición del Servicio

Esto consiste en realizar pruebas, es generar escenarios de pruebas es decir se comparan lo que se esperaba con los resultado reales.(ITIL - Gestión de Servicios TI, 2013)

Para cumplir esto tenemos los siguientes procesos:

- Gestión de la Configuración y Activos
- Gestión del Cambio
- Gestión del Conocimiento
- Planificación y Apoyo a la Transición
- Gestión de Release y Despliegue
- Gestión de Validación y Pruebas
- Evaluación

Operaciones del Servicio

Esto consiste en monitorear activa y pasivamente el funcionamiento del servicio. (ITIL - Gestión de Servicios TI, 2013)

Para cumplir esto tenemos los siguientes procesos:

- Gestión de incidentes
- Gestión de problemas
- Cumplimiento de solicitudes
- Gestión de eventos
- Gestión de accesos

Mejora continua del Servicio

Consiste en utilizar herramientas de medición con el objetivo de documentar la información, que tiene que ver con el funcionamiento del servicio es decir problemas, soluciones y resultados.(ITIL - Gestión de Servicios TI, 2013)

- Los beneficios de utilizar ITIL son:
- Los servicios deben ser consistentes
- Los servicios deben ser repetibles
- Los servicios deben ser auditables
- Los servicios deben ser verificables

Figura 1. Ciclo de Vida de Servicios propuesta por ITIL V3

(Figuerola, 2012)

ITIL no dispone de una metodología de implementación por lo que la implementación depende de la visión o enfoque que la planteen lo importante es determinar las necesidades de la institución ya que implica la automatización de los servicios para lo que se debe analizar ventajas y desventajas de las herramientas que se van a utilizar en dichos procesos.

2.3. COBIT 5

Es un marco de referencia que proporciona buenas prácticas para cumplir los objetivos del negocio alineando las metas estratégicas del negocio con los metas de TI permitiendo ser más competitivos con una correcta institución y administración de TI, brindando un aseguramiento

razonable previniendo, detectando o corriendo eventos no deseados. (ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , 2014).

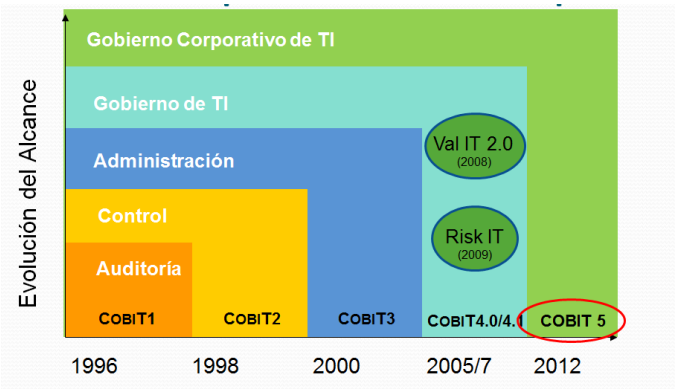

Figura 2. Evolución de COBIT

(ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , 2014)

Dominios

- Evaluar, Orientar y Supervisar
- Alinear, Planificar y Organizar
- Construir, Adquirir e Implementar
- Entregar, dar Servicio y Soporte
- Supervisar, Evaluar y Valorar

Principios de COBIT 5:

COBIT 5 tiene cinco principios que permite construir un marco de referencia enfocado en la gobernanza y la administración eficaz los cuales se describen a continuación.

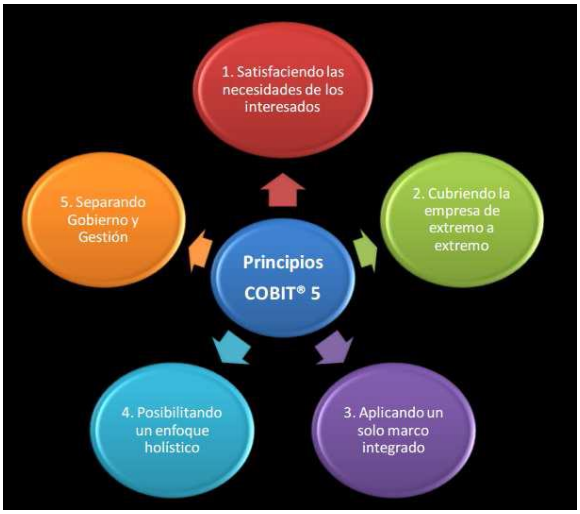

Figura 3. Principios COBIT 5

(ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , 2014)

Satisfacer las necesidades de las Partes Interesadas

Crear valor para las partes interesadas las cuales son consideradas para la toma de decisiones con respecto a la evaluación de riesgos, los beneficios y el manejo de recursos.

Para tomar decisiones se toma en consideración las siguientes preguntas:

¿Quién recibe los beneficios?

¿Quién asume el riesgo?

¿Qué recursos se necesitan?(ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , 2014)

Cubrir la Compañía de Forma Integral

Integra el gobierno de TI con el corporativo de una manera fluida cubriendo todas las funciones y procesos en la institución.(ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , 2014)

Aplicar un solo Marco Integrado

COBIT 5 integra marcos de gobierno y de administración delos cuales se puede mencionar:(ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , 2014)

- Corporativo: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000
- Relacionado con TI: ISO/IEC 38500, ITIL, la serie ISO/IEC 27000, TOGAF, PMBOK/PRINCE2, CMMI

Habilitar un Enfoque Holístico

COBIT necesita una serie de habilitadores de entrada y salida interconectados para cumplir los objetivos principales de la institución.(ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , 2014)

Separar el Gobierno de la Administración

COBIT 5 se basa en los disciplinas de Gobierno y Administración las cuales comprenden diferentes tipos de actividades, estructuras cumpliendo diferentes propósitos. (ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , 2014)

2.4. ADMINISTRACIÓN DE RIESGOS

La Administración de Riesgos es la que debe decidir qué nivel de riesgo está dispuesta aceptar, analiza el nivel tolerable que va aceptar para esto evaluará el costo beneficio.(Castro, 2012)

Por esta razón las organizaciones deben ser conscientes de las vulnerabilidades, conocer los riesgos que enfrenta para poder establecer medidas correctivas y determinar responsabilidades desde un inicio.(Castro, 2012)

Para que se pueda realizar la Administración de Riesgos se requiere de un marco de referencia de las prácticas generalmente aceptadas de control y

seguridad de Tecnología de Información con la finalidad de comparar el ambiente actual con el planeado.(Castro, 2012)

La Administración de Riesgos realiza las siguientes funciones:

- Identifica el riesgo
- Analiza el riesgo
- Valora el riesgo
- Maneja el riesgo

La evaluación de riesgos y vulnerabilidades permite evaluar e identificar los riesgos operativos, haciendo énfasis en los activos de IT Físicos y lógicos de esta forma se incluirá una revisión física de las instalaciones y verificar la seguridad de los elementos físicos y lógicos.(Castro, 2012)

Cada vez se depende más del funcionamiento de los sistemas de información por lo que las empresas se encuentran en constante crecimiento y por lo tanto expuestos a los riesgos informáticos por lo tanto si los sistemas de información sostienen a las empresas en los procesos comercial es esta la razón por la que se debe dar énfasis a los riesgos informáticos que podrían incluir pérdida en la productividad, exposición de datos de los clientes, multas por violación de normas por conservar registros incorrectos, crecimiento de requisitos entre otros.(Castro, 2012)

Para garantizar que una institución administre sus riesgos de la forma adecuada deben definir procesos repetibles para gestionar los riesgos.

Existen varias metodologías de gestión de riesgos como:

- Magerit
- ISO 27005
- Octave o Mehari

De forma general las metodologías constan de los siguientes pasos:

- Identificar y clasificar activos o recursos de la institución
- Evaluar vulnerabilidades, amenazas y probabilidad de ocurrencia

Los métodos de análisis son:

- Cualitativo: clasificaciones descriptivas que describe impactos y probabilidades (Alto, Medio y Bajo)
- Semicuantitativo: están asociados a una escala numérica

Cuantitativo: utilizan valores numéricos para describir probabilidades de impacto

De acuerdo al tipo de riesgo se le puede dar tratamiento:

- Evitar: eliminando el riesgo
- Mitigar: implementar controles para reducir probabilidad e impacto
- Transferir: pasar a otro
- Aceptar: asumir y monitorear

Los beneficios de la administración de riesgos son:

- Priorizar y dar niveles de riesgo a los procesos críticos y no críticos de la institución
- Mitigar el riesgo prevenir las fallas
- Proteger a la institución tomando mejores decisiones
- Evaluar costos de la administración de riesgos
- Estar preparado para auditorías de los entes de control

La administración del riesgo debe lograr un equilibrio del costo entre la aplicación de controles de seguridad y las amenazas realmente significativas.

2.5. AUDITORÍA INFORMÁTICA

Proceso de recolección y evaluación de evidencia para determinar que los sistemas de información cumplen los criterios de seguridad de la información, logran metas organizacionales realizan un uso adecuado de los recursos. (INFORMÁTICA, 2012)

2.6. MARCO CONCEPTUAL

COBIT 5.- Es un marco de referencia que proporciona buenas prácticas para cumplir los objetivos del negocio alineando las metas estratégicas del negocio con los metas de TI permitiendo tener un ambiente de control para una correcta institución y administración de TI, brindando un aseguramiento razonable, previniendo, detectando o corriendo eventos no deseados. (ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , 2014)

Información.-es el activo fundamental en las empresas, representa la principal ventaja competitiva proporcionando apoyo a la alta dirección para la toma de decisiones por lo que las empresas invierten grandes cantidades de dinero, tiempo y esfuerzo para crear sistemas que la administren correctamente, obteniendo productividad y calidad. (ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , 2014)

Seguridad de la Información.-preservación de las siguientes características de información:

- Confidencialidad: Garantizar que información sensitiva sea vista por las accesos autorizadas.
- Integridad: precisión y completitud de la información.
- Disponibilidad: Garantizar el acceso a la información y a los recursos relacionados cuando sea requerida por el negocio
- (ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , 2014)

Auditoria de Sistemas de Información

Proceso de recolección y evaluación de evidencia para determinar que los sistemas de información cumplen los criterios de seguridad de la información, logran metas organizacionales realizan un uso adecuado de los recursos. (ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT , 2014)

Auditoria Basada en Riesgos

Proceso de evaluación que identifica y administra los riesgos de TI que podrían afectar los objetivos de la institución, donde se evalúa la Matriz de Riesgos para determinar el cumplimiento de requisitos técnicos y medios de verificación que permiten determinar los puntos críticos que se deben evaluar en una compañía. (Escalante, 2010)

Norma 410 de Tecnología de la información en Ecuador

Se utilizan para control interno de entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos. (Contraloría General del Estado Ecuatoriano, 2014)

2.7. ESTADO DEL ARTE

A nivel mundial COBIT desde su versión original fue aplicada en varias organizaciones desde entonces existen varias publicaciones, boletines donde se detallan como ha contribuido en aplicaciones de buenas prácticas; tenemos varios casos que a continuación se detallan:

- La Universidad de EAFI en un boletín publicado en el año 2007 hace énfasis en el uso de la herramienta COBIT para gestionar el proceso de auditoría de las compañías, también enfatiza que si se aplica adecuadamente esta herramienta se puede evaluar de forma ágil y consistente el cumplimiento de controles detallados de una institución. (WORLD, 2012)
- *En* América Latinase diferencian en dos grupos las empresas que son reguladas y las que no lo son, el problema radica en las que no son reguladas, ya que alrededor del 80% de estas compañías que no las regularen no usan ningún estándar, las que si quieren mejorar utilizan este estándar COBIT 5 sería una opción muy buena para empezar a utilizar en este grupo que no llevan regulación.(WORLD, 2012)
- Sergio Sperat es socio de Estratega y tiene una trayectoria de más de 20 años como consultor en estrategia de áreas de TI y

negocios, desarrollada en una amplia variedad de industrias en Argentina, Chile, México y Estados Unidos dice en una de sus artículos sobre COBIT 5 hace hincapié que esta herramienta es la única que se ocupa de los controles específicos del área de TI desde una perspectiva del negocio. Al utilizar COBIT 5 y alinearse a los objetivos del negocio hace más simple que los accionistas y gerentes de la compañía puedan alinearse con el área de TI ya que los dos se complementan, es decir van de la mano y se guían.(WORLD, 2012)

CAPITULO III

3. METODOLOGIA DE INVESTIGACION

3.1. UBICACIÓN GEOGRÁFICA DEL PROYECTO DE INVESTIGACIÓN

Sede Principal: se halla ubicado en el Valle de los Chillos en Sangolquí.

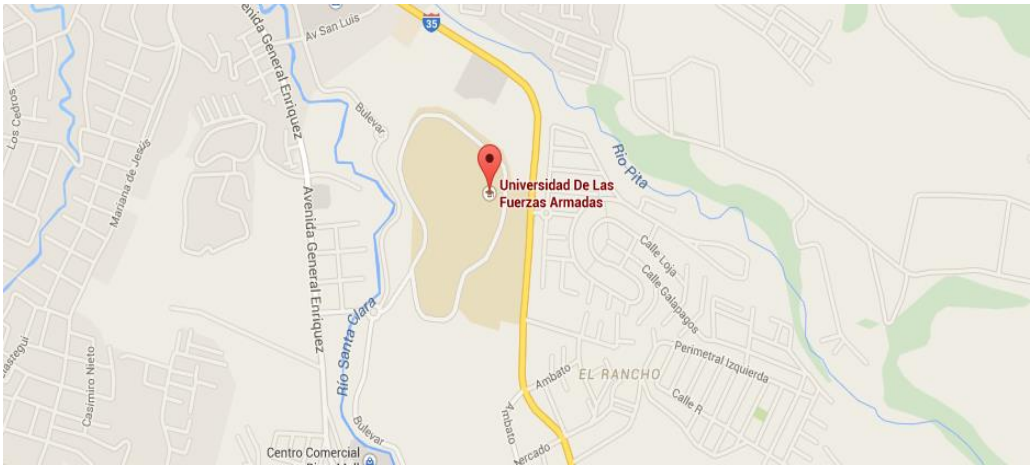

Figura 4. Ubicación Universidad Fuerzas Armadas ESPE

3.2. METODOLOGÍA

De acuerdo al Proyecto de Tesis“Evaluación Técnica Informática de la Planeación y Organización de la ESPE”,se revisócontrolesreferentesalaPlaneaciónyOrganizaciónque actualmente tienen implementados en el departamento de TecnologíadelaInformacióndelaUTIC.

La metodología utilizada fue:

- Recopilación de información mediante entrevistas,cuestionarios.
- Revisión y análisis de documentosdeinformaciónentregadapor la unidad UTIC esto es un respaldo a los cuestionarios ya que es la forma de evidenciar las respuestas a los cuestionarios.

- La información se tabuló, analizó y se detalló en matrices para controlar.

Se partió del Plan Estratégico de la ESPE de este tomamos los objetivos del Plan esto traducido a COBIT representan las necesidades de las partes interesadas, versus las 17 metas de COBIT dimos una ponderación para determinar los objetivos que tienen mayor impacto en las metas de TI ver ANEXO I MATRIZ OBJETIVO VS METAS TI.

Una vez identificadas las metas de TI con ponderaciones más altas se procedió a vincular con los procesos del Dominio Alinear, Planificar y Organizar para identificar los riesgos aceptados para esto se da en la matriz ponderaciones Alto equivalente a 3, 2 medio y 1 bajo ver ANEXOII MATRIZ METAS VINCULADAS DE TI DE COBIT Y LOS PROCESOS ALINEAR, PLANIFICAR Y ORGANIZAR.

Una vez determinados los procesos que tienen mayor riesgo de que no permitan el cumplimiento de las metas corporativas procedemos a tratar los riesgos y determinar qué acciones tomar.

Para analizar a detalle el proceso de Alinear, Planear y Organizar cada proceso se divide en:

- Descripción del proceso son un conjunto de prácticas influenciadas por las políticas de la institución.
- Declaración de Propósito este tiene una descripción del objetivo y la forma en que va a lograr el propósito.
- Objetivos vinculados a las TI son los que se determinaron en la Matriz Objetivo vs Metas TI ver ANEXO II MATRIZ METAS VINCULADAS DE TI DE COBIT Y LOS PROCESOS ALINEAR, PLANIFICAR Y ORGANIZAR.
- Cada objetivo vinculado a las TI se asocia a varias métricas genéricas relacionadas.
- Cada objetivo del proceso está asociado con un conjunto de métricas genéricas

- Cada proceso tiene un conjunto de Prácticas de gestión estas prácticas son guías para alcanzar los objetivos, en la siguiente imagen se visualiza un ejemplo

Tabla I. Práctica de Gestión, entrada/salidas y actividades

PRACTICA DE GESTION				
DESCRIPCION	VIENE DESDE	ENTRADAS	SALIDAS	SALE A
APO07.01 Mantener la dotación de personal suficiente y adecuado.	EDM04.01	Plan de recursos aprobado Principios rectores para la asignación de recursos y capacidades	Evaluaciones de requisitos de personal	Interno
	EDM04.03	Acciones correctivas para hacer frente a las desviaciones de gestión de recursos	Planes de desarrollo de carrera y de competencias	Interno
	APO01.02	Definición de las prácticas de supervisión	Planes de aprovisionamiento de personal	Interno
	APO06.03	Comunicaciones del presupuesto Plan y presupuesto de TI.		
	Fuera del Ámbito de COBIT	Metas y objetivos empresariales Políticas empresariales y procedimientos de RRHH		

- Los procesos están asociados a una matriz genérica RACIA cada tarea, actividad o grupo de tareas se le asigna uno de los roles RACI se detallan los roles.

Tabla II. Estructura Organizativas

ROL / ESCTRUCTURA	DEFINICION/DESCRIPCIONES
DIRECTOR DE INFORMATICA/SISTEMAS (CIO)	Es el ejecutivo de mayor cargo responsable de alinear TI con las estrategias del negocio y que también es responsable de la planificación, de que se disponga de los recursos necesarios del Área de TI y se gestione la entrega de servicios y soluciones de TI para soportar los objetivos de la empresa

Tabla III. Matriz RACI

Se visualiza un ejemplo de las actividades y a qué rol RACI se asignó.

ACTIVIDADES	MATRIZ RACI
1. Valorar los servicios TI actuales y los niveles de servicio para identificar lagunas entre los servicios existentes y los procesos de negocio de los que son base. Identificar áreas de mejora de los servicios existentes y de las opciones de nivel del servicio.	R: Director de Informática/Sistemas (CIO)
2. Analizar, estudiar y estimar la futura demanda y confirmar la capacidad de los servicios TI existentes.	
3. Analizar las actividades de los procesos de negocio para identificar la necesidad de servicios TI nuevos o rediseñados.	
4. Comparar los requisitos identificados con los componentes del servicio existentes en el catálogo. Si es posible, agrupar los componentes del servicio existentes (servicios TI, opciones de nivel de servicio y paquetes de servicios) en nuevos paquetes de servicio para cumplir con los requisitos de negocio identificados.	
5. Siempre que sea posible, relacionar demanda con paquetes de servicio y crear servicios estandarizados para obtener una eficiencia global.	
6. Revisar el catálogo de servicios TI regularmente con la gestión del catálogo y la gestión de relaciones del negocio para identificar servicios obsoletos. Acordar la retirada de los mismos y proponer cambios.	

- Cada práctica de gestión tiene un conjunto de entradas y salidas son los objetos que son necesarios para apoyar la operación del proceso son documentos que certifican respaldan el cumplimiento
- Cada práctica de gestión está asociada a un conjunto de actividades en la siguiente imagen ejemplose muestran las Actividades para la práctica de Gestión del proceso APO07.01 Mantener la dotación del personal suficiente y adecuada.

Tabla IV. Actividades para la práctica de Gestión del proceso APO07.01

ACTIVIDADES
1. Evaluar las necesidades de personal de forma regular o ante cambios importantes para asegurar que: • La función de TI cuenta con recursos suficientes para apoyar de manera adecuada y apropiada las metas • La empresa cuenta con recursos suficientes para apoyar de manera adecuada y apropiada los procesos de negocio y los controles e iniciativas TI.
2. Mantener los procesos de contratación y de retención del personal de TI y del negocio en línea con las políticas y procedimientos de personal globales de la empresa.
3. Incluir controles de antecedentes en el proceso de contratación de TI para empleados, contratistas y proveedores. El alcance y la frecuencia de estos controles dependen de la sensibilidad y/o criticidad de la función.
4. Establecer mecanismos flexibles de dotación de recursos para apoyar a las necesidades cambiantes del negocio, tales como el uso de transferencias, contratistas externos y acuerdos de servicio con terceras partes.
5. Asegurarse de que el entrenamiento cruzado se lleva a cabo y que hay respaldo para el personal clave para reducir la dependencia de una sola persona.

Ver el análisis completo ANEXO IV PRÁCTICAS, ACTIVIDADES Y ENTRADAS/SALIDAS DEL PROCESOS DEL DOMINIO ALINEAR PLANIFICAR Y ORGANIZAR

Se utilizó un cuestionario que consta de 43 preguntas, es un cuestionario cerrado, cada pregunta tiene un documento como sustento para comprobar que las respuestas son válidas, las ventajas de utilizar este tipo de cuestionario son:

- Solicita respuestas breves y específicas de SI/NO
- Es de más fácil respuesta para los encuestados
- Limitan las respuestas de la muestra
- Mantiene al sujeto en el tema.

- Es relativamente objetivo
- Es fácil de clasificar y analizar

VerANEXO V CUESTIONARIO

CAPÍTULO IV

4. INFORME

4.1. RESUMEN EJECUTIVO

El objetivo del presente trabajo es realizar una evaluación a los controles y procesos de las UTIC, en base al dominio de COBIT 5 Alinear, Planificar y Organizar (APO).

Como resultado, se identificóque la constante modificación de la estructura organizacional de la UTIC genera inconvenientes para dar continuidad a los procesos de control existentes, a los que deberían ser implementados y a los que requieren mejora, por lo que se pone en peligro la integridad de información y continuidad del negocio para la Universidad de las Fuerzas Armadas ESPE.

4.2. ALCANCE DE LA AUDITORIA

De acuerdo al presente documento se realizó una auditoria sobre “Evaluación Técnica Informática de la Planeación y Organización de la ESPE Sede Principal” para el período del 1 de Enero del 2014 al 31 de Diciembre del 2014. El alcance de nuestra auditoría consistió en evaluar en base al dominio Alinear, Planear y Organizar (APO) de COBIT 5 al área de UTIC.

La auditoría se basó en los estándares y mejores prácticas de COBIT 5, los cuales requieren que la auditoría sea planeada y realizada mediante la obtención pruebas que sean suficientes, pertinentes y válidas para proporcionar conclusiones y opiniones razonables.

4.3. RESULTADOS DE AUDITORIA

APO07 Gestionar los Recursos Humanos

APO07.01 Mantener la dotación de personal suficiente y adecuado

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-02 Segregación de Funciones que expresa:

"Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.

La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro de la unidad de tecnología de información la supervisión de roles y funciones del personal dentro de cada una de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal.

La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave." (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada "ENCUESTA Nº 1", preguntas Nro.:

2 ¿El personal de TI cuenta con los recursos suficientes para alinearse a los objetivos de la organización?

SI [X] NO [ ]

Se determina que existe un documento en el que detalla una nueva estructura organizacional que no ha sido aprobado para el área de las UTIC “ESTRUCTURA UTIC 2015.pdf”.

Causa:

El documento“ESTRUCTURA UTIC 2015.pdf”, se encuentra en proceso de aprobación.

Efecto:

Control inadecuado en las evaluaciones al personal afectando al cumplimiento de los objetivos institucionales.

Recomendación

Gestionar la aprobación del documento “ESTRUCTURA UTIC 2015.pdf” para poner en marcha el nuevo organigrama.

APO07.02 Identificar personal clave

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-02 Segregación de Funciones que expresa:

“Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.

La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro de la unidad de tecnología de información la supervisión de roles y funciones del personal dentro de cada una de las

áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal.

La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave." (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada "ENCUESTA Nº 1", preguntas Nro.:

4 ¿Tiene manuales de funciones del personal de TI?

SI [X] NO [ ]

Se determina que existe un documentoborrador de funciones del personal que no ha sido aprobado institucionalmente.

Causa:

Documento manual de funciones se encuentra en borrador y no se encuentra aprobado.

Efecto:

Dependencia de personal clave sobre las funciones críticas de la institución.

Recomendación:

Gestionar la aprobación manual de funciones en el que debe estar detalla entrenamiento cruzado.

APO07.03 Mantener las habilidades y competencias del personal

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-15 Capacitación informática que expresa:

"Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. El plan estará orientado a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales." (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada "ENCUESTA Nº 1", preguntas Nro.:

5 ¿Se realiza definición de las habilidades y competencias necesarias del personal de TI y de los recursos externos para que se alineen con los objetivos de la organización?

SI [X] NO [ ]

Se determina la existencia del documento "PLAN DE CAPACITACION UTIC 2014.pdf", donde se muestra una visión general de las capacitaciones que debe hacer el personal pero no se encuentra detallado por habilidades y competencias necesarias para cumplir los objetivos institucionales.

Causa:

Falta de detalle de las capacitaciones que debe realizar el personal, no se encuentra enfocado a las habilidades y competencias.

Efecto:

El personal no se capacita en las habilidades y competencias necesarias para cumplir con sus funciones.

Recomendación:

Mejorar el Plan de Capacitación detallando los cursos de acuerdo a las habilidades y competencias del personal.

APO07.04 Evaluar el desempeño laboral de los empleados.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-02 Segregación de Funciones que expresa:

"Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.

La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro de la unidad de tecnología de información la supervisión de roles y funciones del personal dentro de cada unas de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal.

La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave." (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada “ENCUESTA Nº 1”, preguntas Nro.:

5 ¿Se realiza definición de las habilidades y competencias necesarias del personal de TI y de los recursos externos para que se alineen con los objetivos de la organización?

SI [X] NO [ ]

Se determina que no existe un Plan de Evaluación de desempeño del personal.

Causa:

Falta de evaluaciones formales y periódicas del desempeño.

Efecto:

Estancamiento en el cumplimiento de los objetivos institucionales.

Recomendación:

Crear e implementar un Plan de Desempeño para estimar el desenvolvimiento de los empleados.

APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-02 Segregación de Funciones que expresa:

“Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.

La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro de la unidad de tecnología de información la

supervisión de roles y funciones del personal dentro de cada una de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal.

La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave." (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada "ENCUESTA Nº 1" preguntas Nro.:

3 ¿Se realiza entrenamiento cruzado para el personal clave de TI?

SI [ ] NO [X]

Se determina no existe el Plan de Seguimiento de los recursos humanos.

Causa:

Falta de un proceso de seguimiento de recursos humanos.

Efecto:

Inadecuada gestión sobre la demanda de recursos humanos de las UTIC.

Recomendación:

Crear e implementar el Plan de Seguimiento de Recursos Humanos para las necesidades del área.

APO07.06 Gestionar el personal contratado.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-07 Desarrollo y adquisición de software y aplicativo con la410-08 Adquisiciones de infraestructura tecnológicaque expresa:

410-07 Desarrollo y adquisición de software

“La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

1. La adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. Adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales para: codificación de software, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.

3. Identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales con la participación y aprobación formal de las unidades usuarias. Esto incluye, tipos de usuarios, requerimientos de: entrada, definición de interfaces, archivo, procesamiento, salida, control, seguridad, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en donde aplique.

4. Especificación de criterios de aceptación de los requerimientos que cubrirán la definición de las necesidades, su factibilidad tecnológica y económica, elanálisis de riesgo y de costo-beneficio, la estrategia de

desarrollo o compra del software de aplicación, así como el tratamiento que se dará a aquellos procesos de emergencia que pudieran presentarse.

5. En los procesos de desarrollo, mantenimiento o adquisición de software aplicativo se considerarán: estándares de desarrollo, de documentación y de calidad, el diseño lógico y físico de las aplicaciones, la inclusión apropiada de controles de aplicación diseñados para prevenir, detectar y corregir errores e irregularidades de procesamiento, de modo que éste, sea exacto, completo, oportuno, aprobado y auditable. Se considerarán mecanismos de autorización, integridad de la información, control de acceso, respaldos, diseño e implementación de pistas de auditoría y requerimientos de seguridad. La especificación del diseño considerará las arquitecturas tecnológicas y de información definidas dentro de la institución.

6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor.

7. En los contratos realizados con terceros para desarrollo de software deberá constar que los derechos de autor será de la entidad contratante y el contratista entregará el código fuente. En la definición de los derechos de autor se aplicarán las disposiciones de la Ley de Propiedad Intelectual. Las excepciones serán técnicamente documentadas y aprobadas por la máxima autoridad o su delegado.

8. La implementación de software aplicativo adquirido incluirá los procedimientos de configuración, aceptación y prueba personalizados e implantados. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la institución, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y

los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.

9. Los derechos de autor del software desarrollado a la medida pertenecerán a la entidad y serán registrados en el organismo competente. Para el caso de software adquirido se obtendrá las respectivas licencias de uso.

10. Formalización con actas de aceptación por parte de los usuarios, del paso de los sistemas probados y aprobados desde el ambiente de desarrollo/prueba al de producción y su revisión en la post-implantación.

11. Elaboración de manuales técnicos, de instalación y configuración; así como de usuario, los cuales serán difundidos, publicados y actualizados de forma permanente. ” (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

410-08 Adquisiciones de infraestructura tecnológica

“La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la institución para lo cual se considerarán los siguientes aspectos:

1. Las adquisiciones tecnológicas estarán alineadas a los objetivos de la institución, principios de calidad de servicio, portafolios de proyectos y servicios, y constarán en el plan anual de contrataciones aprobado de la institución, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. La unidad de tecnología de información planificará el incremento de capacidades, evaluará los riesgos tecnológicos, los costos y la vida útil de la inversión para futuras actualizaciones, considerando los requerimientos de carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos. Un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, podrá ser considerado para optimizar los recursos invertidos.

3. En la adquisición de hardware, los contratos respectivos, tendrán el detalle suficiente que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, unidades de entrada/salida, entre otros, y las garantías ofrecidas por el proveedor, a fin de determinar la correspondencia entre los equipos adquiridos y las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual, lo que será confirmado en las respectivas actas de entrega/recepción.

4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la institución contratante."(2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada "ENCUESTA Nº 1" preguntas Nro.:

16 ¿Se dispone de contratos para la adquisición de infraestructuras, instalaciones y servicios relacionados?

SI [X] NO [ ]

De acuerdo al documento "CONTRATO ANTIVIRUS.pdf", facilitado como ejemplo de uno de los contratos se puede identificar que cumple con las condiciones solicitadas para la correcta Gestión del Personal Contratado.

Causa:

Se cumple las especificaciones solicitadas.

Efecto:

Se cumple las especificaciones solicitadas.

Recomendación:

En los contratos desarrollar las cláusulas de control de seguridad de la institución.

APO09 Gestionar los Acuerdos de Servicio

APO09.01 Identificar servicios TI

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-07 Desarrollo y adquisición de software y aplicativo con la410-08 Adquisiciones de infraestructura tecnológicaque expresa:

410-07 Desarrollo y adquisición de software

"La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

1. La adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada. " (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

410-08 Adquisiciones de infraestructura tecnológica

"La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la institución para lo cual se considerarán los siguientes aspectos:

1. Las adquisiciones tecnológicas estarán alineadas a los objetivos de la institución, principios de calidad de servicio, portafolios de proyectos y servicios, y constarán en el plan anual de contrataciones aprobado de la institución, caso contrario serán autorizadas por la máxima autoridad previa

justificación técnica documentada.”(2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada “ENCUESTA Nº 1” preguntas Nro.:

9 ¿Existe un catálogo de servicios de TI? ¿El catálogo de servicios está alineado con los objetivos de la organización?

SI [X] NO [ ]

10 ¿Se encuentra actualizado el catálogo de servicios de TI?

SI [X] NO [ ]

Se determina existe un “CATÁLOGO DE SERVICIOS TIC´S 2014.pdf”.

Causa:

En el Catálogo de Servicios se detallan cada uno de los servicios que dispone la UTIC.

Efecto:

El Catálogo de Servicios contempla los requisitos que dispone la institución.

Recomendación:

El Catálogo de Servicios debe ser revisado de forma periódica.

APO09.02 Catalogar servicios basados en TI.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-07 Desarrollo y adquisición de software y aplicativo con la410-08 Adquisiciones de infraestructura tecnológicaque expresa:

410-07 Desarrollo y adquisición de software

“La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

1. La adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada. ” (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

410-08 Adquisiciones de infraestructura tecnológica

“La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la institución para lo cual se considerarán los siguientes aspectos:

1. Las adquisiciones tecnológicas estarán alineadas a los objetivos de la institución, principios de calidad de servicio, portafolios de proyectos y servicios, y constarán en el plan anual de contrataciones aprobado de la institución, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.”(2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada “ENCUESTA Nº 1” preguntas Nro.:

11 ¿Existe un catálogo de servicios de TI? ¿El catálogo de servicios está alineado con los objetivos de la organización?

SI [S] NO [ ]

12 ¿Se encuentra actualizado el catálogo de servicios de TI?

SI [X] NO [ ]

Se determina existe un “CATÁLOGO DE SERVICIOS TIC´S 2014.pdf”.

De la evaluación realizada se identifican el siguiente documento “CATÁLOGO DE SERVICIOS TIC´S 2014”, permite cumplir con el proceso evaluado.

Causa:

Una correcto Catálogo de servicios basados en TI.

Efecto:

Una correcto Catálogo de servicios basados en TI.

Recomendación:

Realizar revisiones periódicas del Catálogo de servicios basados en TI.

APO09.03 Definir y preparar acuerdos de servicio.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-07 Desarrollo y adquisición de software y aplicativo con la410-08 Adquisiciones de infraestructura tecnológicaque expresa:

410-07 Desarrollo y adquisición de software y aplicativo

"La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor. " (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

410-08 Adquisiciones de infraestructura tecnológica

"La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la institución para lo cual se considerarán los siguientes aspectos:

4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la institución contratante. .”(2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada “ENCUESTA Nº 1” preguntas Nro.:

11 ¿Se establece criterios relativos al tipo, relevancia y criticidad de los contratos y proveedores?

SI [X] NO [ ]

12 ¿Se evalúan los contratos de los proveedores?

SI [X] NO [ ]

13 ¿Disponen de RFIs y RFPs se realizan revisiones?

SI [X] NO [ ]

14 ¿Se dispone de contratos para la adquisición de software?

SI [X] NO [ ]

15 ¿Se obtiene asesoramiento legal sobre acuerdos de adquisición de desarrollos?

SI [X] NO [ ]

16 ¿Se dispone de contratos para la adquisición de infraestructuras, instalaciones y servicios relacionados?

SI [X] NO [ ]

Se hace referencia al documento ejemplo “CONTRATO ANTIVIRUS.pdf”, donde se puede determinar que se definen los acuerdos de servicio.

Causa:

Se cumple el proceso evaluado.

Efecto:

Se cumple el proceso evaluado.

Recomendación:

Realizar revisiones periódicas de acuerdos de los servicios contratados.

APO09.04 Supervisar e informar de los niveles de servicio.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-13 Monitoreo y evaluación de los procesos y servicios que expresa:

“Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

La unidad de tecnología de información definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran.

La unidad de tecnología de información definirá y ejecutará procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos.

La unidad de tecnología de información presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten

acciones correctivas y de mejoramiento del desempeño.”(2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada “ENCUESTA Nº 1” preguntas Nro.:

23 ¿Se realizan encuestas periódicas de calidad por cada uno de los sistemas con los que cuenta la compañía?

SI [X] NO [ ]

24 ¿Existen planes de acciones sobre las encuestas de calidad realizadas a los clientes?

SI [X] NO [ ]

Se determina existe el documento “RESULTADOS ENCUESTAS SERVICIOS TIC´S.pdf” que indica los resultados encuestas servicios Tics generalizada.

Causa:

El documento evaluado “RESULTADOS ENCUESTAS SERVICIOS TIC´S.pdf”, no permite evaluar los niveles de servicio ya que está generalizado.

Efecto:

Al tener una visión generalizada no se pueden realizar planes de acción sobre cada uno de los servicios de los servicios que presta la UTIC.

Recomendación:

Establecer medidas de supervisión para poder tener niveles de servicios adecuados.

APO09.05 Revisar acuerdos de servicio y contratos.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-07 Desarrollo y adquisición de software y aplicativo con la410-08 Adquisiciones de infraestructura tecnológicaque expresa:

410-07 Desarrollo y adquisición de software y aplicativo

"La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor. " (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

410-08 Adquisiciones de infraestructura tecnológica

"La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la institución para lo cual se considerarán los siguientes aspectos:

4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la institución contratante. ."(2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada “ENCUESTA Nº 1” preguntas Nro.:

11 ¿Se establece criterios relativos al tipo, relevancia y criticidad de los contratos y proveedores?

SI [X] NO [ ]

12 ¿Se evalúan los contratos de los proveedores?

SI [X] NO [ ]

Se determina que existe un documento “CATÁLOGO DE PROVEEDORES CONTRATOS 2014.pdf”.

Causa:

El documento “CATÁLOGO DE PROVEEDORES CONTRATOS 2014.pdf”, dispone de la información necesaria para revisar los acuerdos de servicios y contratos.

Efecto:

El Catálogo de Proveedores y contratos facilita la revisión de los contratos discerniendo por proveedor.

Recomendación:

Realizar revisiones periódicas de documento “CATÁLOGO DE PROVEEDORES CONTRATOS 2014.pdf”.

APO10 Gestionar los Proveedores

APO10.01 Identificar y evaluar las relaciones y contratos con proveedores.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-07 Desarrollo y adquisición de software y aplicativo con la410-08 Adquisiciones de infraestructura tecnológicaque expresa:

410-07 Desarrollo y adquisición de software y aplicativo

"La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor. " (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

410-08 Adquisiciones de infraestructura tecnológica

"La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la institución para lo cual se considerarán los siguientes aspectos:

4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la institución contratante. ."(2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada "ENCUESTA Nº 1" preguntas Nro.:

13 ¿Se establece criterios relativos al tipo, relevancia y criticidad de los contratos y proveedores?

SI [X] NO [ ]

14 ¿Se evalúan los contratos de los proveedores?

SI [X] NO [ ]

17 ¿Se realiza gestión de los contratos con los proveedores?

SI [X] NO [ ]

Existe un documento identificado como “CATÁLOGO DE PROVEEDORES CONTRATOS 2014.pdf”, el mismo que nos da una visión general y se evidencia la falta de criterios de tipo, relevancia, criticidad e importancia de cada uno de ellos.

Causa:

La falta de recursos humanos destinados exclusivamente a la gestión de contratos y proveedores.

Efecto:

Asignación inadecuada de los recursos humanos y físicos a procesos críticos, ocasionando deficiencia en el trabajo realizado.

Recomendación:

Al formato actualmente utilizado para la gestión de contratos y proveedores se debe agregar los criterios de tipo, relevancia, criticidad e importancia para cada uno de ellos.

APO10.02 Seleccionar proveedores.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-07 Desarrollo y adquisición de software y aplicativo con la410-08 Adquisiciones de infraestructura tecnológicaque expresa:

410-07 Desarrollo y adquisición de software

“La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

1. La adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. Adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales para: codificación de software, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.

3. Identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales con la participación y aprobación formal de las unidades usuarias. Esto incluye, tipos de usuarios, requerimientos de: entrada, definición de interfaces, archivo, procesamiento, salida, control, seguridad, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en donde aplique.

4. Especificación de criterios de aceptación de los requerimientos que cubrirán la definición de las necesidades, su factibilidad tecnológica y económica, elanálisis de riesgo y de costo-beneficio, la estrategia de desarrollo o compra del software de aplicación, así como el tratamiento que se dará a aquellos procesos de emergencia que pudieran presentarse.

5. En los procesos de desarrollo, mantenimiento o adquisición de software aplicativo se considerarán: estándares de desarrollo, de documentación y de calidad, el diseño lógico y físico de las aplicaciones, la inclusión apropiada de controles de aplicación diseñados para prevenir, detectar y corregir errores e irregularidades de procesamiento, de modo que éste, sea exacto, completo, oportuno, aprobado y auditable. Se considerarán mecanismos de autorización, integridad de la información, control de acceso, respaldos, diseño e implementación de pistas de auditoría y requerimientos

de seguridad. La especificación del diseño considerará las arquitecturas tecnológicas y de información definidas dentro de la institución.

6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor.

7. En los contratos realizados con terceros para desarrollo de software deberá constar que los derechos de autor será de la entidad contratante y el contratista entregará el código fuente. En la definición de los derechos de autor se aplicarán las disposiciones de la Ley de Propiedad Intelectual. Las excepciones serán técnicamente documentadas y aprobadas por la máxima autoridad o su delegado.

8. La implementación de software aplicativo adquirido incluirá los procedimientos de configuración, aceptación y prueba personalizados e implantados. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la institución, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.

9. Los derechos de autor del software desarrollado a la medida pertenecerán a la entidad y serán registrados en el organismo competente. Para el caso de software adquirido se obtendrá las respectivas licencias de uso.

10. Formalización con actas de aceptación por parte de los usuarios, del paso de los sistemas probados y aprobados desde el ambiente de desarrollo/prueba al de producción y su revisión en la post-implantación.

11. Elaboración de manuales técnicos, de instalación y configuración; así como de usuario, los cuales serán difundidos, publicados y actualizados de forma permanente. ” (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

410-08 Adquisiciones de infraestructura tecnológica

“La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la institución para lo cual se considerarán los siguientes aspectos:

1. Las adquisiciones tecnológicas estarán alineadas a los objetivos de la institución, principios de calidad de servicio, portafolios de proyectos y servicios, y constarán en el plan anual de contrataciones aprobado de la institución, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. La unidad de tecnología de información planificará el incremento de capacidades, evaluará los riesgos tecnológicos, los costos y la vida útil de la inversión para futuras actualizaciones, considerando los requerimientos de carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos. Un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, podrá ser considerado para optimizar los recursos invertidos.

3. En la adquisición de hardware, los contratos respectivos, tendrán el detalle suficiente que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, unidades de entrada/salida, entre otros, y las garantías ofrecidas por el proveedor, a fin de determinar la correspondencia entre los equipos adquiridos y las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual, lo que será confirmado en las respectivas actas de entrega/recepción.

4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad

de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la institución contratante.”(2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada “ENCUESTA Nº 1” preguntas Nro.:

15 ¿Se establece criterios relativos al tipo, relevancia y criticidad de los contratos y proveedores?

SI [X] NO [ ]

16 ¿Se evalúan los contratos de los proveedores?

SI [X] NO [ ]

Existe documento identificado como “CATÁLOGO DE PROVEEDORES CONTRATOS 2014.pdf”, en este se detallan los proveedores actuales pero no se cuenta con documentación que haga referencia al proceso de selección para cada uno de ellos.

Causa:

Para la presente evaluación no se identificó con documentación que respalde los procesos de selección de proveedores.

Efecto:

Al no contar con un formato general para la contratación de proveedores los criterios de aceptación son diferentes.

Recomendación:

Generar un formato estándar para el proceso de selección de proveedores.

APO10.03 Gestionar contratos y relaciones con proveedores.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-07 Desarrollo y adquisición de software y aplicativo con la410-08 Adquisiciones de infraestructura tecnológicaque expresa:

410-07 Desarrollo y adquisición de software y aplicativo

"La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor. " (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

410-08 Adquisiciones de infraestructura tecnológica

"La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la institución para lo cual se considerarán los siguientes aspectos:

4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la institución contratante". (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada “ENCUESTA Nº 1” preguntas Nro.:

17 ¿Se realiza gestión de los contratos con los proveedores?

SI ☐ NO ☐

Existe un documento identificado como “CATÁLOGO DE PROVEEDORES CONTRATOS 2014.pdf”, en este se detallan los proveedores.

Causa:

En el documento “CATÁLOGO DE PROVEEDORES CONTRATOS 2014.pdf”, proporciona una visión general de los proveedores existente, pero no se puede determinar su proceso de gestión.

Efecto:

Tener problemas con la gestión de contratos y las relaciones con los proveedores de esta manera.

Recomendación:

Generar un plan para gestionar los contratos y relaciones con proveedores.

APO10.04. Gestionar el riesgo en el suministro.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-11 Plan de contingencias

“Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.” (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada “ENCUESTA Nº 1” preguntas Nro.:

29 ¿Existe una metodología de Identificar los Riesgos de TI?

SI [X] NO [ ]

30 ¿Existe una matriz de Riesgos de TI?

SI [X] NO [ ]

Existe un documento “PLAN_DE_CONTINGENCIA 2014.pdf” que cumple el proceso evaluado.

Causa:

En la evaluación actual el documento PLAN_DE_CONTINGENCIA 2014.pdf” contempla la gestión del riesgo.

Efecto:

Se tiene un control de los posibles problemas con la gestión de riesgos en el periodo de la presente evaluación.

Recomendación:

Actualizar periódicamente el Plan de Contingencia.

APO10.05 Supervisar el cumplimiento y el rendimiento del proveedor.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-07 Desarrollo y adquisición de software y aplicativo con la410-08 Adquisiciones de infraestructura tecnológicaque expresa:

410-07 Desarrollo y adquisición de software y aplicativo

"La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor. " (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

410-08 Adquisiciones de infraestructura tecnológica

"La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la institución para lo cual se considerarán los siguientes aspectos:

4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la institución contratante". (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada "ENCUESTA Nº 1" preguntas Nro.:

11 ¿Se establece criterios relativos al tipo, relevancia y criticidad de los contratos y proveedores?

SI [X] NO [ ]

17¿Se realiza gestión de los contratos con los proveedores?

SI [X] NO [ ]

Existe un documento identificado como “CATÁLOGO DE PROVEEDORES CONTRATOS 2014.pdf”, en este se detallan los proveedores actuales sin especificar los criterios de control a cada uno de ellos.

Causa:

En el documento “CATÁLOGO DE PROVEEDORES CONTRATOS 2014.pdf”, identifica a cada uno de los proveedores pero no la forma de controlar el cumplimiento y el rendimiento de cada uno de ellos.

Efecto:

La información contenida en el documento “CATÁLOGO DE PROVEEDORES CONTRATOS 2014.pdf”, no sea suficiente para tener procedimiento del control del cumplimiento y rendimiento.

Recomendación:

Generar un Proceso de Control de Proveedores donde se detalle los criterios de cumplimiento y rendimiento para cada uno de ellos.

APO11 Gestionar la Calidad

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-13 Monitoreo y evaluación de los procesos y servicios que expresa:

“Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

La unidad de tecnología de información definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran.

La unidad de tecnología de información definirá y ejecutará procedimientos, mecanismos y la periodicidad para la medición, análisis y

mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos.

La unidad de tecnología de información presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño." (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada "ENCUESTA Nº 1" preguntas Nro.:

39 ¿Existe un SGSI de acuerdo a las políticas de la empresa?

SI [X] NO [ ]

40 ¿Existe la autorización de la dirección para implementar y operar o cambiar un SGSI?

SI [X] NO [ ]

Se identifico que existe un borrador de las Políticas de SGC.

Causa:

Falta de oficialización del borrador de Políticas de SGC.

Efecto:

Inefectividad en el trabajo de los colaboradores por no tener claro los procesos de gestión de calidad.

Inadecuada asignación de recursos humanos y físicos a procesos de gestión de calidad para cada uno de los servicios que presta la UTIC.

Recomendación:

Gestionar la aprobación del borrador de Políticas de SGC alineados a los requerimientos institucionales y los servicios presta la UTIC.

APO12 Gestionar el Riesgo

APO12.01 Recopilar datos.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-11 Plan de Contingencias que expresa que:

"Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado".

Condición:

De la encuesta realizada "ENCUESTA Nº 1" preguntas Nro.:

29 ¿Existe una metodología de Identificar los Riesgos de TI?

SI [X] NO [ ]

30 ¿Existe una matriz de Riesgos de TI?

SI [X] NO [ ]

31 ¿Existen datos históricos de los Riesgos de TI?

SI [X] NO [ ]

32 ¿Existe una bitácora de eventos de Riesgos de TI que han causado o pueden causar impactos en el Catalogo de Servicios?

SI [X] NO [ ]

De acuerdo al trabajo realizado se evidencia el "PLAN_DE_CONTINGENCIA 2014.pdf", que es una visión completa sobre la recopilación de riesgos propios.

Causa:

Falta de un estudio sobre datos históricos de riesgo de TI en instituciones con características similares a la ESPE.

Efecto:

La priorización de riesgos se lo haga en base a información histórica propia de la institución sin considerar posibles eventos en instituciones de similares características.

Recomendación:

Establecer un procedimiento para documentar información relacionada con posibles riesgos elaborados en base a eventos similares o a factores que podrían producirlos en instituciones similares a la ESPE.

APO12.02 Analizar el riesgo

Criterio

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-11 Plan de contingencias que expresa que:

"Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado".

Condición:

De la encuesta realizada "ENCUESTA Nº 1" preguntas Nro.:

33 ¿Existe un proceso para la valoración de Riesgos de TI?

SI [X] NO [ ]

34 ¿Con que frecuencia se realiza revisiones Riesgos de TI?

SI [X] NO [ ]

Anual

Trimestral

Mensual

Otro(Especifique)

35 ¿Existe un proceso de identificación y actualización de Riesgos de TI?

SI [X] NO [ ]

De acuerdo al trabajo realizado se evidencia el "PLAN_DE_CONTINGENCIA 2014.pdf", es una visión completa del análisis de riesgos.

Causa

Falta de un estudio sobre datos históricos de riesgo de TI en instituciones con características similares a la ESPE.

Efecto

No contemplar posibles riesgos que pueden afectar la operación de la institución basados en datos de instituciones con características similares a la ESPE.

Recomendación

Realiza un análisis de riesgos basados en datos históricos de posibles eventos que pueden materializarse y producir daños a la institución.

APO12.03 Mantener un perfil de riesgo, APO12.04 Expresar el riesgo, APO12.05 Definir un portafolio de acciones para la gestión de riesgos, APO12.06 Responder al riesgo.

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-11 Plan de contingencias que expresa que:

"Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el

procesamiento de la información por problemas en los equipos, programas o personal relacionado".

Condición:

De la encuesta realizada "ENCUESTA Nº 1" preguntas Nro.:

36 ¿Existe un proceso de Gestión de Riesgo?

SI [X] NO [ ]

37 ¿Existen Planes de Acción de los Riesgos Identificados como críticos de acuerdo a la Matriz de Riesgos?

SI [X] NO [ ]

38 ¿Existe un proceso de valoración de Riesgos de TI?

SI [X] NO [ ]

De acuerdo al trabajo realizado se evidencia el "PLAN_DE_CONTINGENCIA 2014.pdf", es una visión completa del análisis de riesgos.

Causa:

De acuerdo a la evaluación se cumple con el proceso.

Efecto

De acuerdo a la evaluación se cumple con el proceso.

Recomendación:

Mantener revisiones periódicas para mantener el Plan de Contingencia actualizado.

APO13 Gestionar la Seguridad

Criterio:

De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, 410-13 Monitoreo y evaluación de los procesos y servicios que expresa:

“Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

La unidad de tecnología de información definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran.

La unidad de tecnología de información definirá y ejecutará procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos.

La unidad de tecnología de información presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño.” (2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE, 2009)

Condición:

De la encuesta realizada “ENCUESTA Nº 1” preguntas Nro.:

39 ¿Existe un SGSI de acuerdo a las políticas de la empresa?

SI [X] NO [ ]

40 ¿Existe la autorización de la dirección para implementar y operar o cambiar un SGSI?

SI [X] NO [ ]

41 ¿Cómo se comunica los roles y responsabilidades de la gestión de la seguridad de la información?

SI [X] NO [ ]

42 ¿Existe un plan de tratamiento de riesgo de seguridad de la información alineados con los objetivos estratégicos y la arquitectura empresarial?

SI [X] NO [ ]

43 ¿Existe un proceso de Gestión de la Seguridad?

SI [X] NO [ ]

De la encuesta realizada “ENCUESTA Nº 1”, se identifico que existe un borrador de las Políticas de SGC.

Causa:

Falta de oficialización del borrador de Políticas de SGC.

Efecto:

Inefectividad en el trabajo de los colaboradores por no tener claro los procesos de gestión de calidad.

Inadecuada asignación de recursos humanos y físicos a procesos de gestión de calidad para cada uno de los servicios que presta la UTIC.

Recomendación:

Gestionar la aprobación del borrador de Políticas de SGC alineados a los requerimientos institucionales y los servicios presta la UTIC.

4.4. RESUMEN DE RESULTADOS FINALES

Como resultado final de la presente evaluación a la Planeación y Organización de la ESPE sede principal, se detalla un resumen final de nivel de cumplimiento expresado en porcentaje del análisis y recomendacionesrealizadas.

Tabla V. Evaluación cumplimiento APO

PROCESO	SUBPROCESO	Nivel de Cumplimiento por Procesos				
		20% No cumple	40% Mínimo	60% Regular	80% Bueno	100% Excelente
APO07 Gestionar los Recursos Humanos	APO07.01 Mantener la dotación de personal suficiente y adecuado.	X				
	APO07.02 Identificar personal clave de TI.	X				
	APO07.03 Mantener las habilidades y competencias del personal.			X		
	APO07.04 Evaluar el desempeño laboral de los empleados.	X				
	APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.	X				
	APO07.06 Gestionar el personal contratado.	X				
APO09 Gestionar los Acuerdos de Servicio	APO09.01 Identificar servicios TI.					X
	APO09.02 Catalogar servicios basados en TI.					X
	APO09.03 Definir y preparar acuerdos de servicio.			X		
	APO09.04 Supervisar e informar de los niveles de servicio.			X		
	APO09.05 Revisar acuerdos de servicio y contratos.	X				
APO10 Gestionar los Proveedores	APO10.01 Identificar y evaluar las relaciones y contratos con proveedores.				X	
	APO10.02 Seleccionar proveedores.			X		
	APO10.03 Gestionar contratos y relaciones con proveedores.				X	
	APO10.04. Gestionar el riesgo en el suministro.				X	
	APO10.05 Supervisar el cumplimiento y el rendimiento del proveedor.	X				
APO11 Gestionar la Calidad	APO11.01. Establecer un sistema de gestión de la calidad (SGC).		X			

Continua

	APO11.02. Definir y gestionar estándares, procesos y prácticas de calidad.			X		
	APO11.03. Enfocar la gestión de la calidad en los clientes.			X		
	APO11.04. Supervisar y hacer controles y revisiones de la calidad.			X		
	APO11.05. Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.			X		
	APO11.06. Mantener una mejora continua			X		
APO12 Gestionar el Riesgo	APO12.01 Recopilar datos.	X				
	APO12.02 Analizar el riesgo.	X				
	APO12.03 Mantener un perfil de riesgo.				X	
	APO12.04 Expresar el riesgo.				X	
	APO12.05 Definir un portafolio de acciones para la gestión de riesgos.				X	
	APO12.06 Responder al riesgo.				X	
APO13 Gestionar la Seguridad	APO13.01 Establecer y mantener un SGSI.	X				
	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información	X				
	APO13.03 Supervisar y revisar el SGSI.	X				

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Como resultado de la evaluación se constató que los documentos; Nueva Estructura de UTIC y el Manual de Funciones no han sido aprobados, produciendo una incorrecta asignación de tareas en el personal.
- Al disponer de un Plan de Capacitación, Desempeño y Seguimiento sin detallar las habilidades y competencias del personal no permite llevar una adecuada gestión de los recursos humanos disponibles en la UTIC.
- Se determinó que el Catálogo de Servicios detalla correctamente lo servicios disponibles de la UTIC, sin embargo no dispone de medidas de supervisión para tener niveles de servicios adecuados.
- Se verificó que la UTIC ha realizado un gran esfuerzo por tener documentados los contratos y proveedores con los que cuenta, al cual le hace falta agregar criterios de relevancia, criticidad e importancia para mejorar la gestión con los proveedores.
- Se evidenció que uno de los documentos más completos es el Plan de Contingencia ya que cumple con todas los estándares solicitados en la presente evaluación, lo que genera una correcta priorización de servicios, gestión de riesgos y continuidad del negocio.
- Por otro lado el documento SGC disponible en la UTIC es un borrador, no ha sido aprobado, ocasionando que no se puedan realizar mejoras continuas de los servicios que presta la UTIC.

5.2. RECOMENDACIONES

- Gestionar la aprobación de los documentos Nueva Estructura de UTIC , Manual de Funciones, SGC
- Mejorar el Plan de Capacitación, Desempeño y Seguimiento incluyendo las habilidades y competencias del personal
- Realizar encuestas de satisfacción de clientes sobre cada uno de los servicios disponibles en el Catálogo.
- Tabular la información de las encuestas de satisfacción de clientes y aplicar medidas correctivas para mejorar los servicios disponibles de la UTIC.
- Agregar criterios de relevancia, criticidad e importancia al documento de contratos y proveedores.

6. BIBLIOGRAFÍA

(APM), A. f. (2007). *APM Introduction to Programme Management.* Latimer, Trend and Co. GB.

2009, REGISTRO OFICIAL NO. 78 - MARTES 1 DE DICIEMBRE DE. (2009). 410 TECNOLOGÍA DE LA INFORMACIÓN. En *410 TECNOLOGÍA DE LA INFORMACIÓN.*

Benavides., L. C. (2009). *Aplicación de la Norma de Auditoria COBIT en el Monitoreo de Transferencias Eléctronicas de Datos Contables - Financieros.* Barquisimeto.

Castro, A. R. (2012). *Riesgo tecnológico y su impacto para las organizaciones parte II Gobierno de TI y riesgos*. Obtenido de Riesgo tecnológico y su impacto para las organizaciones parte II Gobierno de TI y riesgos: http://revista.seguridad.unam.mx/numero-15/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-ii-gobierno-de-ti-y-riesgos

Contraloría General del Estado Ecuatoriano. (2014). *Contraloria General del Estado*. Obtenido de Dirección de Investigación Técnica, Normativa y de Desarrollo Administrativo: http://www.contraloria.gob.ec/normatividad_vigente.asp

Deloitte. (Abril de 2009). *Deloitte*. Obtenido de http://www.deloitte.com/assets/Dcom-Argentina/Local%20Assets/Documents/arg_cons_ers-VI-ENAI_14052009.pdf

Editores., V. M. (s.f.). 2010.

Escalante, V. M. (2010). *Elementos de Auditoría.* Quinta Edición -Thomson Editores.

Figuerola, N. (2012). *ITIL V3 ¿Por dónde empezar?* . Obtenido de ITIL V3 ¿Por dónde empezar? : https://articulosit.files.wordpress.com/2012/07/itil-v33.pdf

http://es.scribd.com/doc/229413486/Cobit-4-1-vs-Cobit-5. (s.f.).

http://es.scribd.com/doc/229413486/Cobit-4-1-vs-Cobit-5. (s.f.).

http://es.scribd.com/doc/229413486/Cobit-4-1-vs-Cobit-5. (s.f.).

INFORMÁTICA, A. (2012). *AUDITORÍA INFORMÁTICA*. Obtenido de AUDITORÍA INFORMÁTICA: http://members.tripod.com/~Guillermo_Cuellar_M/informatica.html

ISACA. (Noviembre de 2013). *El diagnóstico basado en CobiT*. Obtenido de REPSOL S.A. Dirección de Auditoría de Sistemas.: http://www.isaca.org/chapters7/Madrid/Events/Documents/La%20Funci%C3%B3n%20del%20Diagn%C3%B3stico%20Basado%20en%20CobiT%20en%20la%20Auditor%C3%ADa%20de%20Sistemas%20-%20Erik%20de%20Pablo%20Mart%C3%ADnez.pdf

ISACA. (07 de 2014). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT* . Obtenido de COBIT 5: www.isaca.org

ITIL - Gestión de Servicios TI. (2013). Obtenido de ITIL - Gestión de Servicios TI: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

Pub, V. H. (2012). *COBIT® 5: A Management Guide (Best Practice).*

WORLD, P. (2012). *ISACA presenta COBIT 5 para Seguridad de la Información*. Obtenido de ISACA presenta COBIT 5 para Seguridad de la Información: http://www.pcworld.com.mx/Articulos/23883.htm

7. ANEXOS

ANEXO I. MATRIZ OBJETIVO VS METAS TI.

	Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
1. Valor para los interesados de las inversiones de Negocio	P		P		P	S	P	S	S		P	S	P	S		S	S
2. Cartera de productos y servicios competitivos	P		S		P		P	S	P		S	P	S	S		S	P
3. Riesgos de negocio gestionados (salvaguarda de activos)	S	S	S	P		S	S	S	S	P		S	S	S	S	P	
4. Cumplimiento de leyes y regulaciones externas		P		S			S			P				S	S		
5. Transparencia financiera						P											
6. Cultura de servicio orientada al cliente	P				S		P	S	S			S	S			S	S
7. Continuidad y disponibilidad del servicio del negocio	S			P			S	S		P				P			

Continua

	Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
8. Respuestas ágiles a un entorno de negocio cambiante	P		S	S	S		P		P		S	S				S	P
9.Toma Estratégica de decisiones basadas en información	P		S			S	S	S						P			S
10. Optimización de costes de entrega de servicio	S			P	S	P		S			P	S	S				
11. Optimización de la funcionalidad de los procesos del negocio	P		S		S		P	P	P		S	P		S			S
12. Optimización de los costos de los procesos del negocio	S				P	P	S	S			P	S	S				
13. Programas gestionados de cambio en el negocio	P		P	S			S		S		S	S	P				S
14. Productividad operacional y de los empleados					S			P	S		S	S				P	
15. Cumplimiento con las políticas internas				S						P					P		

Continua

	Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de
16. Personas preparadas y motivadas	S		S	S			S	S	S							P	S
17. Cultura de innovación de producto y negocio	S		S		S		S	S	P		S	S				S	P

ANEXO II. MATRIZ METAS VINCULADAS DE TI DE COBIT Y LOS PROCESOS DE ALINEAR, PLANIFICAR Y ORGANIZAR

	Dominio Alinear, Planificar, Organizar	Alineamiento de TI y la estrategia de negocio	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Agilidad de las TI	Conocimiento, experiencia e iniciativas para la innovación de negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Personal del negocio y de las TI competente y motivado	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Disponibilidad de información útil y relevante para la toma de decisiones	Riesgos de negocio relacionados con las TI gestionados	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Totales
APO03	Administrar la Arquitectura Empresarial	1	1	1	1	1	1	1	1	1	1	1	1	12
APO05	Gestionar la Cartera	1	1	1	1	1	1	1	1	1	1	1	1	12
APO04	Gestionar la Innovación	1	1	3	1	1	1	1	1	1	1	1	1	14
APO08	Gestionar las Relaciones	1	1	1	1	1	3	1	1	1	1	1	1	14
APO01	Gestionar el Marco de TI	3	1	1	1	1	1	3	1	1	1	1	1	16
APO02	Gestionar la Estrategia	3	1	1	1	1	1	3	1	1	1	1	1	16
APO06	Gestionar el Presupuesto y los Costos	1	1	1	3	3	1	3	1	1	1	1	3	20

Continua

	Dominio Alinear, Planificar, Organizar	Alineamiento de TI y la estrategia de negocio	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Agilidad de las TI	Conocimiento, experiencia e iniciativas para la innovación de negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Personal del negocio y de las TI competente y motivado	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Disponibilidad de información útil y relevante para la toma de	Riesgos de negocio relacionados con las TI gestionados	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Totales
APO07	Gestionar los Recursos Humanos	3	1	3	3	1	3	1	3	1	1	1	3	24
APO10	Gestionar los Proveedores	3	3	3	1	1	3	3	3	3	1	3	1	28
APO11	Gestionar la Calidad	1	3	3	3	3	1	3	1	3	1	3	3	28
APO12	Gestionar el Riesgo	3	3	3	3	3	1	3	1	3	1	3	3	30
APO13	Gestionar la Seguridad	3	3	3	3	3	1	3	1	3	1	3	3	30
APO09	Gestionar los Acuerdos de Servicio	3	3	3	3	3	1	3	3	3	3	3	3	34

ANEXO III. PRACTICAS, ACTIVIDADES Y ENTRADAS/SALIDAS DEL PROCESOS DEL DOMINIO ALINEAR PLANIFICAR Y ORGANIZAR

ANEXO IV. CUESTIONARIO

PROYECTO DE EVALUACIÓN TECNICA INFORMÁTICA ESPE

ENCUESTA Nº 1

FUENTE:	Ing. Rommel Astimbay	FECHA DE APLICACIÓN:	22-04-2015	FECHA DE RECEPCIÓN:	22-04-2015	RESPONSABLES:	Ing. Nataly Acuña Ing. Verónica Oguendo

Instrucciones: Es importante que las respuestas al cuestionario sean respaldadas por documentos oficiales, referencias comprobables u otros instrumentos legales que permitan establecer la veracidad de lo expuesto. De lo contrario será considerada solamente como una opinión o comentario personal.

El formulario se provee en formato digital. La fuente deberá entregar al responsable en forma digital e impresa y firmada.

1. ¿Existe un proceso que permita identificar los errores comunes por cada uno de los servicios que presta TI y las posibles soluciones a cada uno de estos errores?
   SI [/] NO [ ]
2. ¿El personal de TI cuenta con los recursos suficientes para alinearse a los objetivos de la organización?
   SI [ ] NO [X]
3. ¿Se realiza entrenamiento cruzado para el personal clave de TI?
   SI [X] NO [ ]
4. ¿Tiene manuales de funciones del personal de TI?
   SI [X] NO [ ]
5. ¿Se realiza definición de las habilidades y competencias necesarias del personal de TI y de los recursos externos para que se alineen con los objetivos de la organización?
   SI [X] NO [ ]
6. ¿Se alinean los objetivos del Área de TI con los objetivos de la organización?
   SI [X] NO [ ]
7. ¿Existen valoraciones de los Servicios TI actuales?
   SI [X] NO [ ]
8. ¿Están los procesos del negocio identificados, diagramados o diseñados?
   SI [X] NO [ ]
9. ¿Existe un catálogo de servicios de TI? ¿El catálogo de servicios está alineado con los objetivos de la organización?
   SI [X] NO [ ]
10. ¿Se encuentra actualizado el catálogo de servicios de TI?
    SI [Y] NO [ ]

11. ¿Se establece criterios relativos al tipo, relevancia y criticidad de los contratos y proveedores?
SI [X] NO [ ] * catalogo de contratos y proveedores.

12. ¿Se evalúan los contratos de los proveedores?
SI [X] NO [ ] Administrativa y técnicas de contrato

13. ¿Disponen de RFIs y RFPs se realizan revisiones?
SI [✓] NO [ ] Service Desk

14. ¿Se dispone de contratos para la adquisición de software?
SI [X] NO [ ] *

15. ¿Se obtiene asesoramiento legal sobre acuerdos de adquisición de desarrollos?
SI [X] NO [ ] Procuraduría y Logística

16. ¿Se dispone de contratos para la adquisición de infraestructuras, instalaciones y servicios relacionados?
SI [X] NO [ ] *

17. ¿Se realiza gestión de los contratos con los proveedores?
SI [X] NO [ ] *

18. ¿Se definen riesgos potenciales en los contratos de servicios? * Talvez
SI [X] NO [ ]

19. ¿Existe un marco de control de TI alineado a los requerimientos empresariales?
SI [X] NO [ ] Cobit 5

20. ¿Existen planes de gestión de la calidad para los procesos importantes?
SI [ ] NO [X] * para gestion de calidad en redes, pero enfocado a productos de TIC's

21. ¿Existe un proceso para medir y supervisar la aceptación de la gestión de calidad y mejorarlo cuando sea necesario?
SI [ ] NO [X] * talvez

22. ¿Frecuencia de revisión de la relevancia, eficiencia y eficacia de los procesos específicos de calidad?

[ ]	Anual
[ ]	Trimestral
[ ]	Mensual
[X]	Otro(especifique) Según el servicio y producto de TIC's

23. ¿Se realizan encuestas periódicas de calidad por cada uno de los sistemas con los que cuenta la compañía?
SI [X] NO [ ] Encuestas Service Desk

24. ¿Existen planes de acciones sobre las encuestas de calidad realizadas a los clientes?
SI [✓] NO [ ] acciones correctivas

25. ¿Con que frecuencia se realiza encuestas de satisfacción del cliente de la calidad de servicios prestados por TI?

	Anual
	Trimestral
	Mensual
X	Otro(especifique)

Según avance o modelos tic's.

26. ¿Existe un equipo de trabajo que valida los criterios de calidad que solicita el cliente?
SI [X] NO [ ]

27. ¿Existen encuestas de satisfacción del cliente sobre la calidad de servicios prestados por TI?
SI [X] NO [ ]

28. ¿Existe una bitácora compartida de las mejores prácticas donde se detalle defectos y errores?
SI [X] NO [ ]

29. ¿Existe una metodología de identificar los Riesgos de TI?
SI [X] NO [ ]

30. ¿Existe una matriz de Riesgos de TI?
SI [X] NO [ ]

31. ¿Existen datos históricos de los Riesgos de TI?
SI [X] NO [ ]

32. ¿Existe una bitácora de eventos de Riesgos de TI que han causado o pueden causar impactos en el Catálogo de Servicios?
SI [X] NO [ ]

33. ¿Existe un proceso para la valoración de Riesgos de TI?
SI [X] NO [ ]

34. ¿Con que frecuencia se realiza revisiones Riesgos de TI?

X	Anual
	Trimestral
	Mensual
	Otro(especifique)

35. ¿Existe un proceso de identificación y actualización de Riesgos de TI?
SI [X] NO [ ]

36. ¿Existe un proceso de Gestión de Riesgo?
SI [X] NO [ ]

37. ¿Existen Planes de Acción de los Riesgos identificados como críticos de acuerdo a la Matriz de Riesgos?
SI [X] NO [ ]

38. ¿Existe un proceso de valoración de Riesgos de TI?
SI [X] NO [ ]

39. ¿Existe un SGSI de acuerdo a los políticas de la empresa?
SI [ ] NO [X]

40. ¿Existe la autorización de la dirección para implementar y operar o cambiar un SGSI?
SI [X] NO [ ]

41. ¿Cómo se comunica los roles y responsabilidades de la gestión de la seguridad de la información?
SI [ ] NO [X]

42. ¿Existe un plan de tratamiento de riesgo de seguridad de la información alineados con los objetivos estratégicos y la arquitectura empresarial?
SI [ ] NO [X] Se va a implementar según Nueva Estándar UTIC 2015

43. ¿Existe un proceso de Gestión de la Seguridad?
SI [ ] NO [X] Se va a implementar según Nuevo Estándar UTIC 2015

Ing. Rommel Asitimbay
Director UTIC

Nataly Acuña
Maestrante

Verónica Ciguencia
Maestrante

¡Gracias por su colaboración!