DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS
VIII PROMOCIÓN

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER.

TEMA:

"EVALUACIÓN TÉCNICA INFORMÁTICA EN BASE DE RIESGOS DE LA ESPE SEDE SANTO DOMINGO, UTILIZANDO EL MARCO DE REFERENCIA COBIT 5"

AUTORES: ING. PAULINA ELIZABETH AYALA BAÑO
ING. MARGOTH ELISA GUARACA MOYOTA

DIRECTOR: ING. RUBEN ARROYO Mgtr
OPONENTE: ING. VICTOR PALIZ M.Sc.

SANGOLQUÍ
2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRIA EN EVALUACIÓN Y SISTEMAS TECNOLOGICOS

CERTIFICADO

Ing. Ing. Víctor Páliz Osorio M.Sc

Ing. Rubén Darío Arroyo Chango Mgtr.

CERTIFICAN

Que el trabajo titulado EVALUACIÓN TÉCNICA INFORMÁTICA EN BASE DE RIESGOS DE LA ESPE SEDE SANTO DOMINGO, UTILIZANDO EL MARCO DE REFERENCIA COBIT 5, realizado por la Ing. Elizabeth Paulina Ayala Baño y por la Ing. Ing. Margoth Elisa Guaraca Moyota, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas de la Universidad de las fuerzas armadas –ESPE.

Debido a que constituye un trabajo que aporta de forma positiva a la gestión que realiza la Universidad de la Fuerzas Armadas ESPE- Sede Santo Domingo, contribuyendo a la mejora continua de los servicios que ofrece al desarrollo de la comunidad, motivo por el cual si recomendamos su publicación.

El mencionado trabajo consta de un empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf).

Además, se autoriza a la Ing. Elizabeth Paulina Ayala Baño y a la Ing. Margoth Elisa Guaraca Moyota, que entregue el presente trabajo al Mgtr. Rubén Darío Arroyo Chango, en su calidad de Director de la Carrera.

Sangolquí, Mayo del 2015

Ing. Rubén Darío Arroyo Chango Mgtr.
DIRECTOR

Ing. Víctor Páliz Osorio M.Sc.
OPONENTE

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRIA EN EVALUACIÓN Y SISTEMAS TECNOLOGICOS

AUTORÍA DE RESPONSABILIDAD

ELIZABETH PAULINA AYALA BAÑO

MARGOTH ELISA GUARACA MOYOTA

DECLARO QUE

El Trabajo de investigación denominado EVALUACIÓN TÉCNICA INFORMÁTICA EN BASE DE RIESGOS DE LA ESPE SEDE SANTO DOMINGO, UTILIZANDO EL MARCO DE REFERENCIA COBIT 5, ha sido desarrollado respetando los derechos intelectuales de terceros, conforme las citas cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de 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. Margoth Elisa Guaraca Moyota,
AUTOR

Ing. Elizabeth Paulina Ayala Baño
AUTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

MAESTRIA EN EVALUACIÓN Y SISTEMAS TECNOLOGICOS

AUTORIZACIÓN

Nosotras, Elizabeth Paulina Ayala Baño y Margoth Elisa Guaraca Moyota.

Autorizamos a la Universidad de las Fuerzas Armadas – ESPE, la publicación en la biblioteca virtual de la Institución del trabajo EVALUACIÓN TÉCNICA INFORMÁTICA EN BASE DE RIESGOS DE LA ESPE SEDE SANTO DOMINGO, UTILIZANDO EL MARCO DE REFERENCIA COBIT 5, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, Mayo 2015.

Ing. Margoth Elisa Guaraca Moyota,
AUTOR

Ing. Elizabeth Paulina Ayala Baño
AUTOR

DEDICATORIA

El presente trabajo dedico a Dios por brindarme la oportunidad de vivir y poder ofrecerme todas estas oportunidades.

A mi familia que son sobre todo mi motor para seguir adelante y mi fortaleza, los amo.

Elizabeth Ayala

A ti mi Mateo, hijo querido, por ser mi más grande motivación y razón de vivir, a ti Daniel, por apoyarme en lo que has podido y cuidar de nuestro hijo en mi ausencia, a ti mamita por todo tu apoyo incondicional y a toda mi familia, sobre todo gracias a ti mi Dios por darme todas las oportunidades y ser mi guía en el camino.

Magolhy

AGRADECIMIENTO

Aylen, mi pequeña niña, ahora aun no lo entiendas, pero te agradezco por haberme brindado la oportunidad de ser tu madre, enseñarme que es la felicidad y estar conmigo todas estas noches. Javier, mi amado esposo, lo logramos, esto es tan tuyo como mío, gracias por todo tu apoyo, amor incondicional y sobre todo tu paciencia. Te amo y siempre te amare.

Mis Longos, gracias sin ustedes no lo hubiera logrado, estoy segura que si hay un cielo, ustedes después de esta vida los encontrare ahí. Mis loquitas, todo su tiempo brindado para mí y mi hija permitió que hoy este donde estoy. Gracias infinitas. Las amo con todo mi corazón.

Magui, amiga de lucha, gracias por dejarme ser tu compañera en este proyecto y brindarme tu amistad incondicional, y tu apoyo.

Mis Llamingos y compañeros gracias por su amistad sin su ayuda no lo hubiera logrado.

Elizabeth Ayala

Un Especial Agradecimiento a Universidad de la Fuerzas Armada ESPE, por habernos permitido formar parte de esta gran institución y adquirir nuevos conocimientos.

A la ESPE sede Santo Domingo, por habernos abierto las puertas y permitir realizar el presente trabajo. Al Mg. Eduardo Benavides por brindarnos todas las facilidades e información que permitió la culminación de este proyecto. Al Tcrn. Agr. Efrén Cisneros por brindarnos su valioso tiempo y colaboración.

Al Mg. Mario Ron, por ser el mentor del macro proyecto del que forma parte nuestro trabajo, por todo su compromiso y responsabilidad.

Al Ing. Rubén Arroyo nuestro Director de tesis, por su gran colaboración, disposición y guía en la realización de cada una de las etapas de este trabajo.

Margoth y Paulina

ÍNDICE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Actualmente las instituciones educativas del país deben cumplir con procedimientos de evaluación y acreditación emitidos por el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior. (CEAACES), que tiene por objetivo asegurar una educación de calidad, la Universidad de las Fuerzas Armadas ESPE, actualmente está trabajando para poder alcanzar los estándares necesarios de Acreditación, para ello aprobó el proyecto "Evaluación Técnica Informática de la Universidad de las Fuerzas Armadas ESPE" del cual forma parte este proyecto, el objetivo principal es la ejecución de una Evaluación Técnica Informática basada en riesgos al área de Tecnología de la ESPE sede Santo Domingo utilizando el Marco de Referencia COBIT 5. La metodología aplicada para ejecutar la evaluación técnica consta de 3 fases: La primera fase es el estudio preliminar donde se conoce la entidad a evaluar, se elabora el plan de auditoría, que contiene el alcance, objetivos, cuestionarios, solicitudes y demás documentos necesarios, la siguiente fase es la ejecución de la evaluación donde se realiza la revisión de los procesos , controles, seguridades, documentos, políticas y procedimientos relacionados, además se realizan, pruebas de cumplimiento que ayudan a establecer los procesos críticos o que no estén alineadas a los objetivos estratégicos de la institución, y por último la etapa final donde se publica un informe de auditoría con los hallazgos, criterios de valuación, causa, riesgos y las respectivas recomendaciones de cada proceso evaluado. Los resultados servirán para que de forma objetiva apliquen los controles necesarios que mitigue los riesgos relevantes que pueden estar amenazando al normal funcionamiento de la Universidad.

PALABRAS CLAVE:

- **COBIT 5,**
- **EVALUACIÓN INFORMATICA,**
- **PLAN DE AUDITORIA,**
- **INFORME DE AUDITORÍA**.
- **RIESGOS**

ABSTRACT

Nowadays, the educational institutions in the country have to fulfill with the evaluation and accreditation procedures submitted by the Consejo de Evaluación, Acreditación and Aseguramiento de la Calidad de Educación Superior (CEAACES), which has as aim to guarantee quality in education, the Universidad de las Fuerzas Armadas ESPE, actually is working to achieve the necessary standards for the Accreditation, for which the project "Technical Computing Evaluation of the Universidad de las Fuerzas Armadas ESPE" was approved, the main aim is the carrying out of an Technical Computing Evaluation based on the risks on the Technological area at the ESPE sede Santo Domingo using the Reference Framework COBIT 5. The methodology applied to carry out the technical evaluation includes 3 stages. The first stage is the initial study, which allowed knowing the institution to be evaluated, the auditory plan is made, which includes the reach, objectives, questionnaires, requests and other necessary documents, the next stage is the carrying out stage, in which the processes, controls, securities, documents, politics and procedures inspection are checked, in addition, the observance tests useful to establish the critical processes or those which are not according to the strategic objectives of the institution, finally, the last stage includes an audit report with the finds, evaluation criteria, cause, risks and the respective recommendations of each evaluated process. The results will be used in order to apply objectively the necessary controls to reduce the relevant risks that might threaten the appropriate development of the University.

KEY WORDS:

- **COBIT 5,**
- **COMPUTER EVALUATION,**
- **AUDIT PLAN,**
- **FINAL REPORT.**
- **RISKS**

1. ASPECTOS GENERALES

1.1. Antecedentes

La Universidad de las Fuerzas Armadas – ESPE, forma parte del Sistema de Educación Superior del Ecuador, es una institución que posee autonomía administrativa, personería jurídica y patrimonio propio, de derecho público, está compuesta por: la sede matriz está ubicada en la provincia de Pichincha, ciudad Sangolquí, la sede ESPE Latacunga ubicada en Provincia de Cotopaxi, ciudad Latacunga y ESPE Santo Domingo ubicada en la provincia Santo Domingo de los Tsáchilas, ciudad Santo Domingo, la institución está regida por la Ley Orgánica de Educación Superior (LOES), Estatuto aprobado por el Consejo de Educación Superior (CES) y demás reglamento internos. Su misión es formar académicos y profesionales de excelencia; generar, aplicar y difundir el conocimiento y, proponer e implementar alternativas de solución a problemas de interés público en sus zonas de influencia, su visión es ser líder en gestión del conocimiento y de la tecnología en el Sistema de Educación Superior, con prestigio Internacional y referente de práctica de valores éticos, cívicos y de servicio a la sociedad.

Actualmente la Universidad de las Fuerzas Armadas del Ecuador – ESPE, se encuentra en un proceso de Evaluación y Acreditación y para eso se han ejecutado varios cambios a nivel institucional entre ellos, el modelo educativo, estructura organizacional y procesos de gestión institucional.

La ESPE sede Santo Domingo es parte importante de la institución porque contribuye al desarrollo de la región formando profesionales entregados y responsables en la carrera de Ingeniería Agropecuaria (IASAII), uno de los factores clave para el desarrollo de la institución es la Unidad de Tecnologías de Información y Comunicación porque facilita por medio del uso de las TIC el proceso de enseñanza aprendizaje a los estudiantes, además permite centralizar y administrar los procesos administrativos y académicos de forma adecuada. La ESPE Santo Domingo está entrando a un proceso de cambio, acreditación y ampliación de la oferta académica lo que significaría que se debe fortalecer el área de TI.

A nivel general en la institución se encuentra aprobado el Proyecto para la Evaluación Técnica Informática de la Universidad de las Fuerzas Armadas ESPE, que desarrolla el Vicerrectorado General, el mismo que permitirá conocer de forma imparcial el estado actual de los procesos Gobierno de TI, además permitirá emitir las respectivas recomendaciones basadas en las mejores prácticas que ofrecen Marcos de Referencia como COBIT 5, ISO, entre otros.

Para que la evaluación sea integral se realizará el proyecto denominado Evaluación Técnica Informática en base de riesgos de la ESPE Sede Santo Domingo, utilizando el marco de referencia COBIT 5, la misma que permitirá determinar procesos críticos, verificar controles y si el área de TI está alineada con los objetivos estratégicos institucionales.

La ejecución de este proyecto no solo permitirá un control interno más eficaz de la Unidad de Tecnologías y Comunicación de la ESPE Sede Santo Domingo, sino que también contribuirá a cumplir con los requerimientos demandados por el CEAACES.

1.2. Justificación e importancia

1.2.1. Estado del arte a nivel mundial y local

En un mundo globalizado como el de hoy la mayoría de organizaciones sufren rápidos cambios tecnológicos ya sea para brindar un mejor servicio o para cumplir con normas o estándares que le permita a la empresa mantenerse en el mercado y seguir siendo competitiva, al estar en constante cambio de nuevas tecnologías estos cambios traen asociados ciertos riesgos que incluso podrían poner en peligro la existencia de la organización debido a esto las empresas buscan conocer esos riesgos; dentro de sus posibilidades mitigarlos y proponer planes de acción que permita a la empresa en su momento aplicarlos; y que la empresa afronte exitosamente esos riesgos o amenazas.

El objetivo de TI es apoyar a la organización a alcanzar sus objetivos estratégicos para lograr estos objetivos existen varios marcos de referencia y estándares internacionales que brindan buenas practicas permitiendo alinear los

objetivos de TI con los de la organización, COBIT 5 ofrece un marco integral con varios objetivos de control que orientan y ofrecen un modelo de referencia aplicable para la gestión de TI, es decir ayuda a las empresas a crear valor mediante un balance entre la obtención de beneficios y la optimización de los niveles del riesgo y el uso de recursos, además permite administrar de forma integral cubriendo todo el negocio de extremo a extremo teniendo en cuenta a los grupos de interés.

En el Ecuador, las organizaciones están conscientes de los riesgos asociados a los rápidos cambios tecnológicos ya que sus operaciones en la mayorías de los casos están apoyadas en plataformas tecnológicas debido a esto contratan a empresas que realizan consultorías de evaluaciones técnicas y auditorías informáticas las misma que permiten detectar los riesgos, mejorar e implementar nuevos controles que permitan garantizar la seguridad de la información, establecer responsabilidades y sobre todo alinearse con los objetivos del negocio.

Las instituciones de educación superior no son ajenas a estos cambios y más ahora que están sujetas a evaluaciones y acreditaciones en las que el objetivo es elevar la calidad de la educación bajo leyes de orden regulatorio que deben ser cumplidos para lograr la acreditación esto es controlado desde entidades como la Secretaria Nacional de Educación Superior Ciencia y Tecnología y el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior, el área de TI debe estar orientada a ayudar a cumplir con los requerimientos e indicadores de calidad académica con una plataforma tecnológica que soporte los procesos de gestión y evaluación.

Santo Domingo de los Tsáchilas no se encuentra al margen del proceso de regulación y acreditación, en la actualidad en la provincia están instituciones con gran renombre y trayectoria como la Universidad Tecnológica Equinoccial, la Pontificia Universidad Católica del Ecuador Sede Santo Domingo, la Universidad Central del Ecuador y la ESPE Sede Santo Domingo, las mismas que desempeñan sus tareas de índole operativa con sus diferentes ofertas académicas a los estudiantes de la región.

1.3. Planteamiento del problema

La Universidad de las Fuerzas Armadas ESPE es una universidad comprometida con la educación y la sociedad, para poder brindar el servicio de educación de calidad a la sociedad tiene el Campus Matriz y sus respectivas sedes: ESPE sede Latacunga, Escuela de Ciencias Tecnológicas Héroes del Cenepa y ESPE sede Santo Domingo, los cuales están obligados a cumplir con los procesos de evaluación y acreditación, para lograr el objetivo deben cumplir con estándares e indicadores de calidad que exige el gobierno.

La ESPE sede Santo Domingo, en vista de la necesidad de cumplir con los requerimientos de evaluación y acreditación, requiere de una evaluación técnica a su unidad de tecnología la misma que permitirá detectar riesgos y vulnerabilidades permitiendo de esta forma emitir recomendaciones de control y contingencia que permitan mitigar el riesgo y minimizar el impacto si el riesgo se ha materializado en un problema, además se debe verificar que los objetivos de TI estén alineados a los de la ESPE Matriz.

Históricamente la Universidad de las Fuerzas Armadas ESPE, no ha tenido ningún tipo de auditoría oficial por lo que resulta imperioso realizar una evaluación técnica de cada una de las unidades de tecnología que conforman la universidad ya sea en la Matriz o sus respectivas sedes, este proyecto forma parte macro proyecto de evaluación en base de riesgos de la Universidad de las Fuerzas Armadas ESPE, persigue evaluar al área de tecnología de la ESPE Sede Santo Domingo, basándose en una auditoría basada en riesgos en conjunto con el estándar internacional COBIT 5 de modo que se logre una evaluación integral que permita emitir recomendaciones acertadas y oportunas para el beneficio la institución.

1.4. Objetivo General

Ejecutar una Evaluación Técnica Informática basada en riesgos al área de Tecnología de la Universidad de las Fuerzas Armadas ESPE sede Santo Domingo utilizando el Marco de Referencia COBIT 5, con el fin de determinar las medidas de

control apropiadas para que el área de tecnología ofrezca un servicio acorde a las necesidades de la comunidad universitaria.

1.5. Objetivos Específicos

- Elaborar el Plan de investigación de campo que permita recopilar información que muestre la situación actual del área de tecnología de la ESPE Sede Santo Domingo.

- Diseñar el Plan de Auditoría en el que se definirá los objetivos, puntos a evaluar y los instrumentos de evaluación.

- Ejecutar el Plan de Auditoría elaborado previamente que permita identificar los riesgos tecnológicos usando los procesos de TI basados en COBIT 5.

- Presentar un informe con las recomendaciones pertinentes con controles y procedimientos que ayuden a mitigar el riesgo detectado en los procesos del área de tecnología.

2. FUNDAMENTACIÓN TEÓRICA

2.1. Organización

La Universidad de las Fuerzas Armadas – ESPE, es una institución de educación superior de calidad que ofrece sus servicios a la sociedad ecuatoriana, como toda organización tiene su estructura Organizacional el mismo que permite establecer jerarquías, responsabilidades y vías de comunicación e información.

La estructura organizacional vigente de la Universidad de las Fuerzas Armadas – ESPE hasta la presente fecha es la que se indica a continuación:

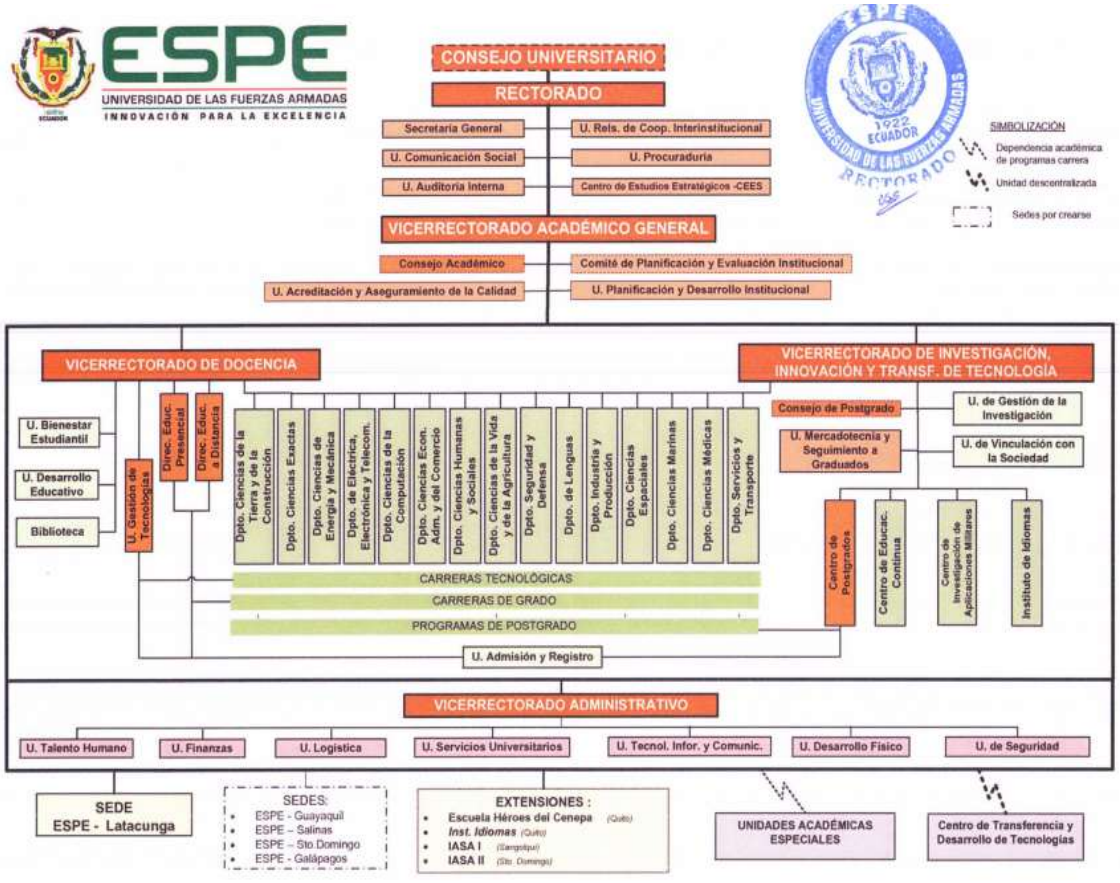

Figura 1. Organigrama ESPE

Fuente: (www.espe.edu.ec, 2014)

La estructura Organizacional permite cumplir las metas organizacionales planteados en la planificación estratégica de la misma, la Planificación Estratégica de

la Universidad de las Fuerzas Armadas – ESPE, está dada bajo un enfoque de Sistemas y Procesos. La planificación estratégica se puede ver en el **Anexo 1**. A continuación se presenta el mapa estratégico de la universidad.

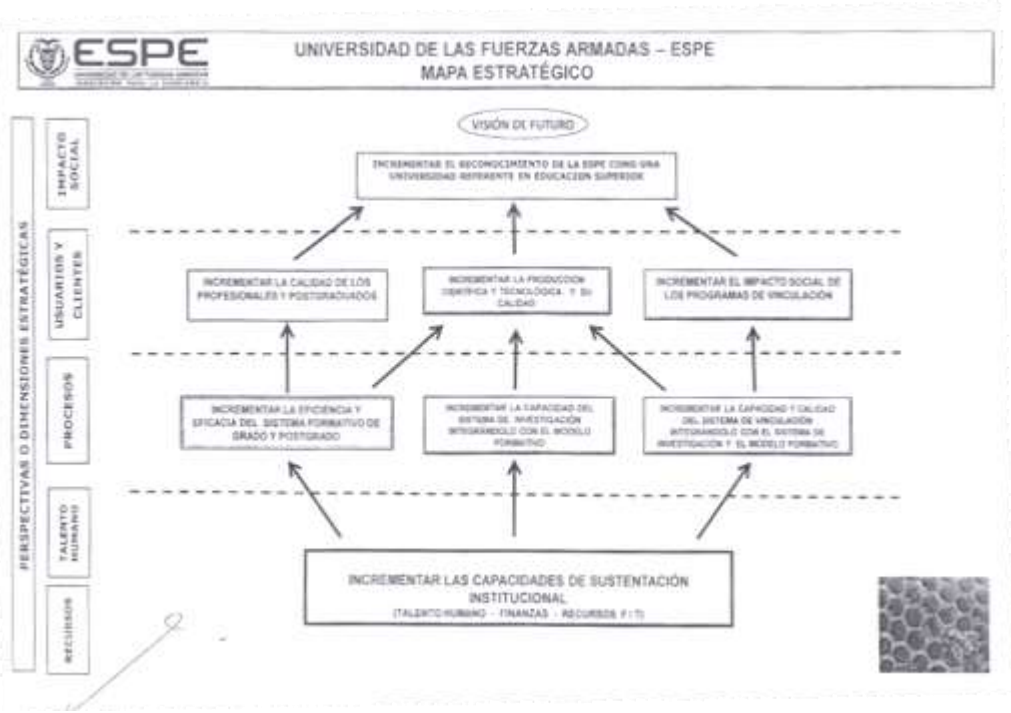

Figura 2. Mapa Estratégico ESPE

Fuente: (www.espe.edu.ec, 2014)

.

2.1.1. ESPE – Santo Domingo

La Carrera de Ingeniería en Agropecuaria Santo Domingo de la Universidad de las Fuerzas Armadas ESPE, se presenta como una alternativa en la enseñanza agropecuaria del país e invita a los bachilleres interesados en el agro a formar parte de este grupo selecto de estudiantes y optar por una Carrera de Futuro, en instalaciones de primera y con docentes especializados que pondrán a su disposición sus más altos conocimientos y su mejor experiencia para aportar en la formación profesional.

Figura 3. ESPE Sede Santo Domingo

Fuente: (**www**.espe.edu.ec, 2014)

A continuación en la figura 4 se muestra la estructura organizacional de la Espe Santo Domingo donde se observa dos grandes subdivisiones ; el consejo de Carrera y la Jefatura administrativa, pero no se encuentra una area de TI especifica.

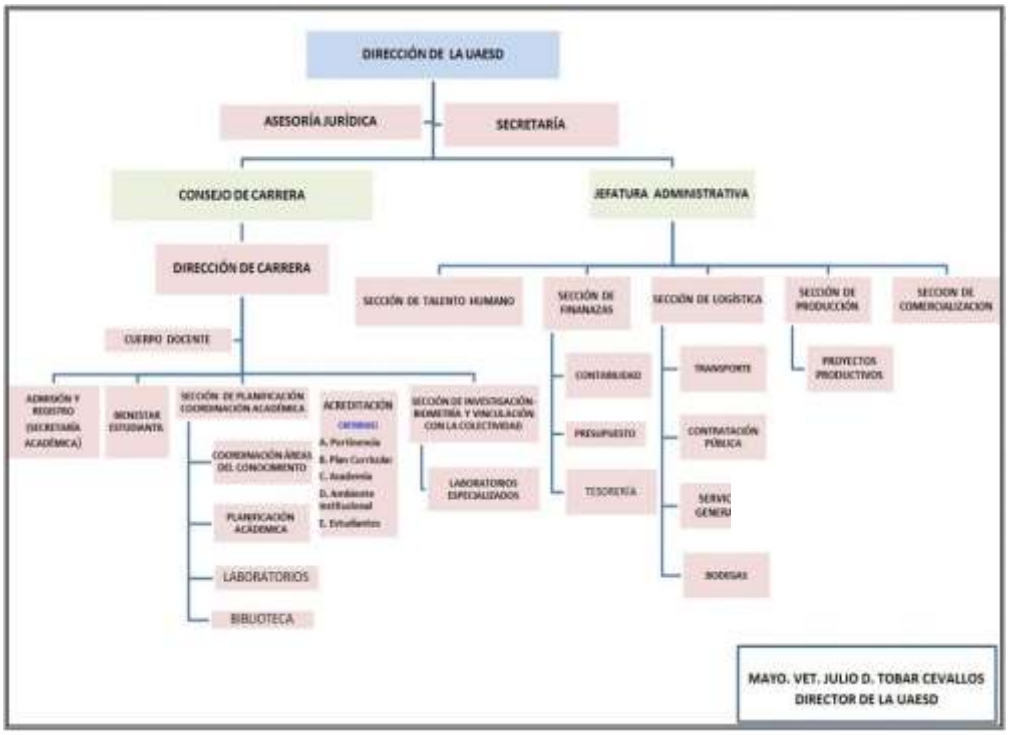

Figura 4. Organigrama de la ESPE Santo Domingo

Fuente: (www.espe.edu.ec, 2014)

2.2. Auditoría

A continuación se detallan algunas definiciones de autores de auditoría:

La palabra auditoría viene de latin auditorius, y de ésta proviene la palabra auditor la misma que significa que tiene la virtud de oír, el diccionario lo define como "revisor de cuentas auditor". EL auditor tiene la virtud de oír y revisar cuenta, pero debe estar encaminado a un objetivo específico que el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de recursos alternativos de acción, se tome decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la actuación". (Piattini & Del Peso, 2001)

Para Hernández la auditoría es un proceso necesario para las organizaciones con la finalidad de proteger y asegurar de forma adecuada sus activos. En donde, la alta dirección espera que de los procesos auditados salgan las recomendaciones acertadas para la mejora continua de las funciones de la organización. (Hernández Hernández, 2002)

Para Pattini, la auditoría, es la actividad que consiste en emitir una opinión profesional sobre si el objeto sometido a análisis demuestra de forma adecuada la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas. (Piattini & Del Peso, 2001).

Existen varios tipos de auditoría pero el que interesa es la auditoría informática que se define a continuación

2.3. Auditoría Informática

Es importante revisar la definición de auditoría informática porque en eso consiste el objetivo del proyecto:

La auditoría informática es el conjunto de técnicas, procedimientos para evaluar y controlar un sistema informático, cuyo fin es validar si sus actividades son correctas y están enmarcadas dentro de los lineamientos de la organización. (Quishpe Goyes & Vargas Cisneros, 2013).

Pattini sostiene que la Auditoría Informática es un proceso que consiste en recoger, agrupar y evaluar evidencias que permita comprobar si un sistema informático protege los activos, mantiene la integridad de los datos, realiza de forma eficaz los fines de la organización, además utiliza eficientemente los recursos. (Piattini Velthius, del Peso Navarro, & del Peso Ruiz, 2008).

2.4. Enfoque Basado en Riesgos

Al realizar una evaluación o auditoria basada en riesgos el auditor debe entender la entidad y debe identificar y analizar los riesgos relevantes para alcanzar los objetivos y determinar las actividades de control. Para plantear y ejecutar procedimientos de auditoría que respondan a los riesgos valorados y reduzcan a un nivel aceptable

Según Ergio Choy Esta Metodología basada en riesgos facilita y mejora la calidad de auditoría, transforma el proceso de Auditoría tradicional en una nueva estructura para evaluar de qué manera se administra los riesgos del negocio de una compañía, además permite adquirir un entendimiento integral del negocio, sus objetivos, sus riesgos, sus procesos.

2.4.1. Funciones de Auditoria Basada en Riesgos

Para Ergio Choy las funciones de una auditoria basada en riesgos son:

- Incorporar al universo de los asuntos de auditoría la visión de riesgo que tiene la organización.
- Desarrollar procesos de auditoría basada en riesgos e incorporarlos en los planes anuales de la auditoría.
- Darle seguimiento al plan estratégico y ajustar el plan de la auditoría ante cambios en el primero.
- Utilizar técnicas y procedimientos de riesgo cuando se realiza la auditoría.

- Informar a los administradores y responsables de la organización los resultados delas auditorías con un lenguaje de riesgos y no de control interno.

- Identificar de manera conjunta los riesgos que pudieran afectar adversamente la continuidad de la organización para alcanzar sus objetivos.

- Ayudar a evaluar el Impacto que pudieran tener estos riesgos dentro de la organización.

- Sugerir el tratamiento y/o las acciones que deberán establecerse para disminuir la probabilidad de exposición a estos riesgos.

- Evaluar la suficiencia y efectividad de los controles internos actuales.

- Obtener planes de acción de los responsables para corregir las fallas de control identificadas.

Dar a conocer los resultados a la Dirección General y a su Comité de Auditoría, mediante reporte de auditoría redactado adecuadamente, basado en los hallazgos de auditoría para una oportuna y adecuada toma de decisiones.

2.5. COBIT 5

ISACA desarrollo una guía de nueva generación COBIT 5 que es un marco de trabajo que permite a todo tipo de organizaciones, tanto pequeñas como grandes, tanto comerciales, como sin ánimo de lucro o del sector público, lograr sus objetivos para el gobierno y la gestión de las TI corporativas. COBIT 5 es un apoyo para que las empresas puedan crear valor, manteniendo el equilibrio entre el uso de recursos, la generación de beneficios y la optimización de los niveles de riesgo con TI.

Actualmente es muy importante abarcar al negocio completo de principio a fin, tomar especial interés en las áreas fundamentales que permiten la continuidad y considerar las necesidades de las partes interesadas (Internas y Externas) del negocio

esto se puede dar mediante la gobernabilidad y gestión de un modo holístico de TI que lo permite COBIT 5.

Los cinco principios claves para el gobierno y gestión de TI en que se basa COBIT 5 son los siguientes:

Figura 5. Principios de COBIT 5.
Fuente: (ISACA 2012)

2.5.1. Principio 1. Satisfacer las Necesidades de las Partes Interesadas

"Creación de valor significa conseguir beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo". (ISACA, 2012). Todas las empresas están concebidas para generar valor ya sea para los accionistas, clientes, o empleados y este valor se pueden presentar de muchas formas como beneficio de servicio, beneficio financiero entre otros.

Por la naturaleza propia de las empresas existe diferentes partes interesadas y generar valor tiene un significado diferente y muchas veces contradictorios entre ellas. Es donde interviene la palabra Gobierno, las actividades de gobierno lo que busca es negociar y decidir entre los diferentes intereses y el valor a generar de las partes interesadas.

Figura 6. El objetivo de Gobierno: Creación de Valor

Fuente: (ISACA 2012)

Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.

"COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas." (ISACA, 2012)

2.5.1.1. Cascada de Metas de COBIT 5

Cada empresa necesita un sistema de gobierno y gestión personalizado debido a que opera a contextos diferentes, que viene determinados por factores internos (organización, la cultura, umbral de riesgo, etc.) y externos (el mercado, la industria, políticas, etc.).

"La cascada de metas de COBIT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI y metas catalizadoras específicas, útiles y a medida. " (ISACA, 2012)

La cascada de metas es muy importante para la empresa porque permite determinar las prioridades de implementación, mejora y aseguramiento del gobierno de TI mediante las metas corporativas, metas relacionadas con las TI y su riesgo relacionado.

2.5.2. Principio 2: Cubrir la Empresa Extremo-a-Extremo

Para COBIT 5 el gobierno y la gestión de la información y la tecnología es desde una perspectiva extremo a- extremo y para toda la empresa, permitiendo: Integrar el gobierno de TI en el gobierno corporativo, sin importar el tipo de gobierno y alineado a las ultimas visiones.

Cubrir todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas, contemplando todos los servicios de TI internos y externos importantes, así como los procesos de negocio, COBIT 5 puede lograr todo esto basado en varios catalizadores.

"Los catalizadores son para toda la empresa y extremo-a-extremo, es decir, incluyendo todo y a todos; internos y externos, que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionada, incluyendo las actividades y responsabilidades tanto de las funciones TI como de las funciones de negocio." (ISACA, 2012)

2.5.2.1. Enfoque de Gobierno

La base de COBIT 5 es el enfoque de gobierno de extremo a extremo, a continuación se presenta los componentes claves:

Figura 7. Gobierno y Gestión en COBIT 5

Fuente: (ISACA 2012)

2.5.3. Principio 3: Aplicar un Marco de Referencia único integrado

Actualmente en el mercado se puede encontrar muchos estándares y buenas prácticas relacionados a TI, cada uno de ellos enfocados o especializados en subgrupos de actividades de TI. COBIT 5 es un estándar que se puede alinear con cualquiera de ellos pero a un alto nivel permitiéndole ser el marco de trabajo primordial para el gobierno y la gestión de las TI de la organización.

Según ISACA (2012) COBIT 5 proporciona a sus grupos de interés la guía más completa y actualizada sobre el gobierno y la gestión de la empresa TI mediante:

- La investigación y utilización de un conjunto de fuentes que han impulsado el nuevo contenido desarrollado, incluyendo:
- La unión de todas las guías existentes de ISACA (COBIT 4.1, Val IT 2.0, Risk IT, BMIS) en este único marco.
- Completar este contenido con áreas que necesitaban más elaboración y actualización.
- El alineamiento a otros estándares y marcos relevantes, tales como ITIL, TOGAF y estándares ISO.
- Definiendo un conjunto de catalizadores de gobierno y gestión que proporcionan una estructura para todos los materiales de guía.
- Poblando una base de conocimiento COBIT 5 que contiene todas las guías y contenido producido hasta ahora y que proporcionará una estructura para contenidos futuros adicionales. (ISACA, 2012).

2.5.4. Principio 4: Hacer Posible un Enfoque Holístico

Para que sea efectivo y eficiente la gestión y gobierno de TI, es necesario un enfoque holístico, donde los catalizadores (*enablers*) sirven de apoyo para la implementación del sistema de gobierno y gestión global para las TI de la empresa.

Lo que debe conseguir los catalizadores lo definen los objetivos relacionados con

TI, los mismo que están guiados por la cascada de metas.

Según ISACA (2012) El marco de referencia COBIT 5 describe siete categorías de catalizadores:

- **Principios, políticas y marcos de referencia** son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.

- Los **procesos** describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.

- Las **estructuras organizativas** son las entidades de toma de decisiones clave en una organización.

- La **Cultura, ética y comportamiento** de los individuos y de la empresa son muy a menudo subestimados como factor de éxito.

- La **información** impregna toda la organización e incluye toda la información producida y utilizada por la empresa.

- Los **servicios, infraestructuras y aplicaciones** incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.

- Las **personas, habilidades y competencias** están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades. (ISACA, 2012)

Figura 8. Catalizadores Corporativos

Fuente: (ISACA 2012)

2.5.5. Principio 5: Separar el Gobierno de la Gestión

Para el marco de trabajo COBIT 5 el gobierno y gestión son dos disciplinas que engloban diferentes tipos de procesos, necesitan estructuras organizativas diferentes y sirven a diferentes propósitos.

Según ISACA (2012) Gobierno. Asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas. La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales. (ISACA, 2012).

3. EVALUACIÓN TÉCNICA INFORMÁTICA

3.1. Metodología

La Metodología utilizada para la evaluación técnica informática a la ESPE Sede Santo Domingo, está dado bajo los siguientes parámetros: métodos y técnicas de investigación, el Marco de Referencia COBIT 5. En base a estos parámetros se realiza la planeación de la auditoría y según el esquema obtenido se realiza la ejecución de la misma y en función de los hallazgos se emiten las respectivas recomendaciones en el informe final.

3.2. Planeación de la evaluación

Se realiza la planificación de la evaluación en base a un análisis de la situación actual de la institución, el mismo que se realiza por medio de la observación directa del lugar a ser evaluado en donde se determinan los objetivos, el alcance y cronograma de las actividades a realizar, las principales actividades a realizar para el trabajo de auditoría son los siguientes:

1. Investigar y analizar información referente a COBIT 5 y riesgos informáticos.

2. Recabar y analizar la información referente a la parte tecnológica de la ESPE – Santo Domingo.

3. Determinar los procesos más críticos y relevantes en base a los objetivos estratégicos de la ESPE, que serán objeto de la evaluación.

4. Ejecutar la auditoria en base a los procesos y actividades preseleccionadas con COBIT 5, dichos procesos basados en los objetivos estratégicos de la institución.

5. Analizar los riesgos presentes de la parte tecnológica de la institución.

6. Elaborar el informe de la evaluación técnica informática en base a los riesgos encontrados.

3.2.1. Objetivos de la evaluación

3.2.1.1. Objetivo General

Realizar una evaluación técnica informática a la parte tecnológica de la ESPE – Sede Santo Domingo en base a riesgos utilizando como marco de referencia COBIT5.

3.2.1.2. Objetivos específicos

- Valorar la situación actual del área tecnológica de la ESPE – Sede Santo Domingo.
- Determinar los procesos críticos en base a COBIT 5, los mismos que serán evaluados.
- Ejecutar la evaluación técnica informática de la situación actual de la parte tecnológica de la ESPE – Sede Santo Domingo con respecto a lo que recomienda COBIT 5 de los procesos seleccionados.
- Realizar el informe final de auditoria con los riesgos encontrados y formular sus concernientes recomendaciones pertinentes en base al modelo COBIT 5 para las no conformidades respectivas.

3.2.2. Alcance de la evaluación

Evaluación técnica de los procesos críticos del área tecnológica de la ESPE – Sede Santo Domingo, se aplicará el modelo en cascada de COBIT 5 para determinar los procesos críticos que deberán ser evaluados, y de estos procesos se escogerán las actividades más importantes con sus respectivas entradas y salidas; las mismas que serán evaluadas en la ejecución de la auditoría, finalmente se elaborará un informe de auditoría basado en riesgos de los hallazgos obtenidos y las respectivas recomendaciones.

3.2.3. Equipo auditor

Ing. Paulina Ayala, Ing. Margoth Guaraca

3.2.4. Comprensión del negocio y sus procesos de negocio

La Universidad de las Fuerzas Armadas tiene como principal objetivo ser un referente dentro de las instituciones educativas en todo el país, para lo cual es necesario que toda la institución se una para alcanzar este objetivo planteado, por lo tanto es necesario realizar una evaluación a toda la universidad para potencializar sus servicios que actualmente brinda.

"Para producir es necesario abandonar las oficinas, internarse en el campo, ensuciarse las manos y transpirar; es el único lenguaje que entienden la tierra, las plantas y los animales". Este pensamiento de Norman Burlaug sintetiza la razón de ser de esta joven Carrera de la ESPE en Santo Domingo: una institución entregada a la formación del recurso humano que el campo necesita para su desarrollo y para generar trabajo y riqueza en beneficio de la comunidad (Burlaung, 2014).

Esta es la filosofía de la Universidad de la Fuerzas Armadas ESPE- Santo Domingo, la misma que ofrece la Carrera de Ingeniería Agropecuaria II Santo Domingo conocida como IASA II, entidad a la que se le realizara la evaluación, está compuesta por dos campus universitarios uno en el kilómetro 24 de la vía a Quevedo en la que están las dependencias administrativas y otro campus en el kilómetro 35 de la vía a Quevedo, en el mismo que están las dependencias académicas y laboratorios. Para poder obtener información de primera mano y comprender de mejor manera el proceso de negocio, se realizó una visita de observación preliminar; donde se pudo determinar que no hay área de Tecnologías de Información, existe un docente el mismo que por encargo interno es el responsable de los laboratorios de cómputo que posee la institución. En base a esta observación preliminar y acorde a la planeación estratégica de la Universidad de las Fuerzas Armadas – ESPE, se elaboraron los objetivos y el alcance de la auditoría.

Desde aquí se partirá para realizar un análisis con la ayuda del marco de referencia COBIT 5 y el personal de la institución, que determinaran los procesos con mayor criticidad dentro de la parte tecnológica de la ESPE Santo Domingo.

3.2.4.1. Entrevista Preliminar:

A continuación se detallan las preguntas aplicadas en la entrevista preliminar realizada al Ing. Eduardo Benavides, encargado de los laboratorios de la ESPE Sede Santo Domingo.

- ¿La sede tiene un área de Tecnología (TI)?
- ¿La sede tiene un plan estratégico informático?
- En caso afirmativo. ¿Conoce el plan estratégico institucional?
- ¿Cuáles son los objetivos a largo plazo?
- ¿Cuáles son los objetivos a mediano plazo?
- ¿Cuáles son los objetivos corto plazo?
- ¿Se mantienen las estructuras procesos y prácticas?
- ¿Tiene claro sus responsabilidades y autoridad?
- ¿Existen políticas, normas del departamento de tecnología
- ¿Existen planes de contingencia para el área informática?
- En el caso de tenerlo ¿cómo se las comunica a los demás áreas?
- ¿Existen manuales de procedimientos de los sistemas?
- ¿Cómo se realiza la adquisición de la infraestructura tecnológica?
- ¿Actualmente existen proyectos que serán implementados en el área?
- ¿Anualmente o periódicamente se realiza un presupuesto y se lo asigna a la unidad informática?
- ¿Con qué tipo de seguridades lógicas cuenta la información de la sede?

- ¿Con qué tipo de seguridades físicas cuenta la información de la sede?
- ¿Con qué tipo de seguridad física se cuenta en las oficinas?
- ¿Hay mantenimiento periódico al software y hardware?
- ¿Se realizan capacitaciones a los usuarios de los sistemas informáticos?
- ¿Cuántas personas trabajan en el área de TI?
- ¿Cuál es el tiempo que labora en la institución y en el puesto que actualmente se desempeña?
- ¿Cuántas veces ha recibido su computadora un mantenimiento preventivo por cada año?
- ¿Puede recuperar sus datos, por alguna falla o se borran?
- ¿La red de datos está siempre disponible?
- ¿Cómo optimiza los procesos para obtener resultados con costo aceptables?
- ¿Cómo se asegura que los servicios que se brindan en la institución sol los que se oferta?
- ¿Las capacidades de las personas, procesos y tecnologías soportan los objetivos de la empresa?
- ¿Cómo se gestiona la información y el uso de los recursos de TI?
- ¿Qué procesos se realiza para responder a los objetivos estratégicos?
- ¿Cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI?
- ¿Qué actividades se desarrollan dentro de la institución que permitan optimizar las capacidades del personal?

- ¿Cómo relaciona los objetivos de la institución con los objetivos del área?
- ¿Qué proveedores para el área de TI posee?
- ¿Qué área administra los proveedores de TI?
- ¿Cuándo surgen problemas o incidentes como se resuelve?

Al momento que se realiza la entrevista es necesario sustentar dicha información con documentos de los procesos de la institución.

3.2.4.2. Documentos a Solicitar

En una auditoria es primordial la presentación de documentos que respalde la información recabada, por lo tanto en necesario solicitar documentos, a continuación se cita algunos de ellos, el Anexo 7 es el documento en el cual se detallan los documentos, solicitudes y la disponibilidad de los mismos en la institución:

- Plan estratégico ESPE Sede Santo Domingo.
- Políticas de la institución.
- Manuales de procesos y procedimientos.
- Documentos sobre los equipos, series y características y todo sobre los mismos.
- Manual de los procedimientos de los sistemas.
- Proyectos de instalación de nuevos sistemas.
- Registro de copia de respaldo de datos Sede Santo Domingo.
- Inventario actualizado de equipos de cómputo y de red.
- Diagrama de cableado estructurado de la red de telefonía y datos de la ESPE Sede Santo Domingo

- Listado de activos de Equipos de cómputo y de Red ESPE Sato Domingo.
- Documento de Políticas normas de uso de laboratorios ESPE Sede Santo domingo
- Listado de activos de equipos de cómputo y de red y los responsables de los mismos, ESPE Sede Santo Domingo.

3.2.5. Cumplimiento (Normas internas y Externas)

La Universidad de las Fuerzas Armadas – ESPE, al ser una institución de Educación Superior está regida por la Ley de Educación Superior (LOES) y su respectivo reglamento, de igual forma hasta que el Estatuto de la Universidad de las Fuerzas Armadas sea aprobado por la Secretaría de Educación Superior, se encuentra vigente el Estatuto, Reglamentos, Normas y Disposiciones administrativas y financieras aprobados hasta la actualidad.

3.3. Ejecución de la evaluación

3.3.1. Selección de los procesos críticos a evaluar

Esta auditoria "EVALUACIÓN TÉCNICA INFORMÁTICA EN BASE DE RIESGOS DE LA ESPE SEDE SANTO DOMINGO, UTILIZANDO EL MARCO DE REFERENCIA COBIT 5." Forma parte del proyecto de "EVALUACIÓN TÉCNICA INFORMÁTICA DE LA ESPE" por tal razón el proceso que a continuación se detalla parte desde la planificación estratégica (Plan Estratégico 2014-2017) ANEXO 1, fuente que nos brinda las metas de la organización y el alineamiento que tiene la institución para estos próximos años.

A continuación se detallan los objetivos Estratégicos con sus respectivas estrategias:

- **OBJETIVO ESTRATÉGICO 1 - OE 1:**

  Incrementar el reconocimiento de la Universidad de las Fuerzas Armadas - ESPE como una institución referente en educación superior.

ESTRATEGIAS:

1. Alcanzar estándares nacionales e Internacionales de calidad.
2. Implementar nuevas alianzas estratégicas con entidades académicas nacionales e internacionales.
3. Desarrollar eventos de difusión de actividades y resultados logrados en los programas de investigación y vinculación.
4. Implementar alianzas de cooperación con gobiernos locales y entidades de los sectores productivos para impulsar el desarrollo de las zonas de influencia
5. Mejorar y ampliar la participación en proyectos comunitarios en las zonas de influencia.

- **OBJETIVO ESTRATÉGICO 2 - OE 2:**

Incrementar la calidad de los profesionales y postgraduados.

ESTRATEGIAS:

1. Actualizar periódicamente los estudios de demanda y pertinencia de las carreras y programas de postgrado, para adecuar la oferta académica de la Universidad
2. Crear e implementar nuevas relaciones de cooperación académica de la Universidad con los sectores productivos y sociales.
3. Desarrollar y ampliar las actividades de investigación y vinculación social de los estudiantes de tercer y cuarto nivel.

- **OBJETIVO ESTRATÉGICO 3 - OE 3:**

Incrementar la producción científica - tecnológica y su calidad.

ESTRATEGIAS:

1. Generar programas y proyectos de investigación con alto impacto.
2. Crear modelos y prototipos de Interés para las zonas de influencia.

3. Generar libros y publicaciones de impacto, indexados a nivel internacional.
4. Desarrollar programas de especialización y maestrías de investigación intercolaborativos.
5. Crear programas de doctorado.

- **OBJETIVO ESTRATÉGICO 4 - OE 4:**

Incrementar el impacto social de los programas de vinculación.

ESTRATEGIAS:

1. Actualizar la oferta de servicios de la universidad hacia la comunidad.
2. Implementar modelos y prototipos desarrollados por la universidad en las zonas de influencia.
3. Generar programas de apoyo al emprendimiento productivos en las zonas de influencia.
4. Implementar programas educativos para grupos vulnerables en las zonas de influencia.
5. Incrementar el número de proyectos estudiantiles en las zonas de influencia.

- **OBJETIVO ESTRATÉGICO 5 - OE 5:**

Incrementar la eficiencia y eficacia del sistema formativo de grado y postgrado.

ESTRATEGIAS:

1. Innovar el modelo formativo, Orientado al desarrollo de competencias.
2. Mejorar las competencias del personal académico.
3. Actualizar la oferta de carreras de grado en áreas específicas del conocimiento.
4. Actualizar la oferta de programas de postgrado.

5. Implementar programas de cuarto nivel conjuntamente con otras universidades, nacionales e internacionales.
6. Mejorar los procesos de formación articulados con las líneas de investigación y sus respectivos grupos, en las áreas de vinculación en las zonas de influencia.

- **OBJETIVO ESTRATÉGICO 6 - OE 6:**

Incrementar la capacidad del sistema de investigación integrándolo con el modelo formativo.

ESTRATEGIAS:

1. Incrementar el número de investigadores titulares (PhD).
2. Implementar grupos y redes de investigación multidisciplinarios con investigadores internos y externos.
3. Implementar la infraestructura física y tecnológica para el desarrollo de la investigación.
4. Generar un ambiente que promueva e impulse la investigación y facilite la movilidad.
5. Mejorar los procesos de investigación articulados a la formación y vinculación.
6. Enviar a los investigadores a participar en proyectos de investigación conjunta en universidades extranjeras para publicación de los resultados en revistas o libros indexados.

- **OBJETIVO ESTRATÉGICO 7 - OE 7:**

Incrementar la capacidad y calidad del sistema de vinculación integrándolo con el sistema de investigación y con el modelo formativo.

ESTRATEGIAS:

1. Incrementar la participación de estudiantes y profesores en actividades vinculación con la sociedad.
2. Mejorar el sistema de vinculación con la sociedad.

3. Mejorar los procesos de vinculación articulados a la formación y la investigación orientados a aplicar alternativas de solución en las zonas de Influencia.

- **OBJETIVO ESTRATÉGICO 8 - OE 8:**

  Incrementar las capacidades de sustentación institucional. (Talento Humano- Finanzas- Recursos Físicos y Tecnológicos).

  ESTRATEGIAS:

  1. Mejorar la gestión del talento humano.
  2. Mejorar la eficiencia y eficacia en la gestión presupuesta.
  3. Generar mayor cantidad de recursos financieros por autogestión
  4. Renovar y desarrollar la infraestructura física y tecnológica de apoyo a la gestión académica y administrativa.

Para determinar los procesos que se tomaron en cuenta en la evaluación fue necesario referirse a los objetivos y estrategias de la ESPE señalados en el Plan Estratégico de la ESPE 2014 – 2017, y se conjuga con las 14 metas empresariales establecidas en COBIT 5, se realizó una tabla donde en las columnas se colocaron todos las estrategias y en las filas todas las Metas Empresariales que tiene COBIT 5 y se procedió a dar un peso de acuerdo al nivel de alineamiento que tiene cada estrategia con las metas empresariales de COBIT 5, de acuerdo a la Tabla 01, que se muestra a continuación:

Tabla 01

Valoración para las estrategias ESPE

PESO	DESCRIPCIÓN
0	No está alineada la estrategia de la ESPE con la meta empresarial de COBIT
1	Parcialmente alineada la estrategia de la ESPE con la meta empresarial de COBIT
2	Alineada la estrategia de la ESPE con la meta empresarial de COBIT

Fuente: Los Autores

La actividad la realizo dos grupos; el primer grupo conformado por personal que labora en la ESPE Matriz, encabezado por el Ing. Rommel Asitimbay Director de la UTIC y personal de la UTIC, esta evaluación está representada con el 70% del valor total debido a que estas personas están el día a día en la universidad y saben la realidad de la misma. El segundo grupo fueron los auditores del proyecto de evaluación de la ESPE, del que forma parte esta tesis, estos puntos representaron el 30% del puntaje total.

En la Tabla 02 se tiene las 17 metas empresariales de COBIT 5, con su puntaje final, la meta empresarial que se encuentra más alineadas con las estrategias de la ESPE es la 1 “Valor para los interesados de las inversiones de Negocio” cuyo valor llega al 73, siendo el valor más alto que sirve de referencia para la selección de las demás metas. Después de analizar y seleccionar las de mayor valor, se obtuvo 13 metas corporativas que están marcadas con la letra P y sirven para seguir en la selección de los procesos a evaluar. Esta tabla representa un resumen de todos los pasos realizados para determinar los procesos a ser evaluados. En el Anexo 2 Tabla de Selección de Procesos, se puede observar de manera detallada cada uno de los pesos y los asignados para el resultado final.

Tabla 02

Relación Estrategias ESPE- Metas Empresariales COBIT 5

GRUPO DE AUDITORES Y PERSONAL DE LA ESPE	FINAL	METAS SELECCIONADAS
METAS EMPRESARIALES COBIT 5		
1. Valor para los interesados de las inversiones de Negocio	73,00	P
2. Cartera de productos y servicios competitivos	67,95	P
3. Riesgos de negocio gestionados (salvaguarda de activos)	37,65	P
4. Cumplimiento de leyes y regulaciones externas	39,48	P
5. Transparencia financiera	25,25	S
6. Cultura de servicio orientada al cliente	55,55	P
7. Continuidad y disponibilidad del servicio del negocio	46,83	P
8. Respuestas ágiles a un entorno de negocio cambiante	63,82	P
9.Toma Estratégica de decisiones basa en información	36,27	P
10. Optimización de costes de entrega de servicio	29,84	S
11. Optimización de la funcionalidad de los procesos del negocio	39,03	P
12. Optimización de los costos de los procesos del negocio	33,97	S
13. Programas gestionados de cambio en el negocio	37,00	P
14. Productividad operacional y de los empleados	43,16	P
15. Cumplimiento con las políticas internas	30,30	S
16. Personas preparadas y motivadas	50,96	P
17. Cultura de innovación de producto y negocio	64,74	P

Fuente: Los Autores, (ISACA, 2012)

Ya seleccionadas las metas corporativas de COBIT 5, y siguiendo el modelo de cascada, el siguiente paso es determinar las Metas de TI, por medio de la relación de las metas empresariales anteriormente elegidas y las metas de TI de COBIT,

utilizando la tabla ‘’Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI’’ del documento de ISACA de COBIT 5.

En dicha tabla se sustituyeron los las letras P y S por los valores 3 y 1, para luego sumar los valores de cada una de las metas de TI, las metas que presentaban mayores puntajes fueron las seleccionadas.

Tabla 03

Metas Empresariales COBIT 5 - Metas TI COBIT 5

METAS EMPRESARIALES METAS TI	1. Valor para los interesados de las inversiones de Negocio	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de leyes y regulaciones externas	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio del negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9.Toma Estratégica de decisiones basadas en información	11. Optimización de la funcionalidad de los procesos del negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	16. Personas preparadas y motivadas	17. Cultura de innovación de producto y negocio	SUMATORIA	PUNTAJE
Alineamiento de TI y la estrategia de negocio	3	3	1		3	1	3	3	3	3		1	1	25	100
Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			1	3										4	16
Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	3	1	1				1	1	1	3		1	1	13	52
Riesgos de negocio relacionados con las TI gestionados			3	1		3	1			1		1		10	40
Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	3	3			1		1		1		1		1	11	44
Transparencia de los costes, beneficios y riesgos de las TI	1		1					1						3	12
Entrega de servicios de TI de acuerdo a los requisitos del negocio	3	3	1	1	3	1	3	1	3	1		1	1	22	88
Uso adecuado de aplicaciones, información y soluciones tecnológicas.	1	1	1		1	1		1	3		3	1	1	14	56
Agilidad de las TI	1	3	1		1		3		3	1	1	1	3	18	72
Seguridad de la información, infraestructura de procesamiento y aplicaciones			3	3		3								9	36
Optimización de activos, recursos y capacidades de las TI	3	1					1		1	1	1		1	9	36
Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	1	3	1		1		1		3	1	1		1	13	52
Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	3	1	1		1					3				9	36
Disponibilidad de información útil y relevante para la toma de decisiones	1	1	1	1		3		3	1					11	44
Cumplimiento de las políticas internas por parte de las TI			1	1										2	8
Personal del negocio y de las TI competente y motivado	1	1	3		1		1				3	3	1	14	56
Conocimiento, experiencia e iniciativas para la innovación de negocio	1	3			1		3	1	1	1		1	3	15	60

Fuente: Los Autores, (ISACA, 2012)

En la Tabla 03 se puede observar que la comparación arrojó 13 objetivos de TI, los objetivos de TI que están resaltados de color anaranjado son los que se

excluyeron por presentar menor valor, aunque se tomó en cuenta las metas "Seguridad de la información, infraestructura de procesamiento y aplicaciones" y la meta "Optimización de activos, recursos y capacidades de las TI" por su importancia en el negocio aunque presente un puntaje relativamente bajo De los objetivos seleccionados el de mayor relevancia es "Alineamiento de TI y la estrategia de negocio" cuyo valor asciende al 100.

El último paso para seleccionar los procesos para la evaluación es relacionar las metas de TI anteriormente seleccionadas con los procesos de TI en la tabla "Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos", donde se reemplazó las letras P y S por valores 3, 1, respectivamente; para luego proceder a la suma de cada uno de los procesos.

En la Tabla 04 se encuentran los 39 procesos de TI, y el valor que arrojaron después de una comparación con las metas de TI anteriormente seleccionadas, el valor máximo de la sumatoria fue 21 que equivale al 100%, los procesos que serán evaluados en este proyecto serán los mayores a 14 (70%), se escogió este valor porque con ello se seleccionó 17 procesos de los 39, que es un valor considerable.

Tabla 04

Metas TI COBIT 5-Procesos

	PROCESOS COBIT 5	SUMATORIA METAS TI	PUNTAJE
Evaluar, Orientar, Supervisar	01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.	18	85,7
	02 Asegurar la entrega de beneficios.	18	85,7
	03 Asegurar la optimización del riesgo.	13	61,9
	04 Asegurar la optimización de recursos.	16	76,2
	05 Asegurar la transparencia hacia las partes interesadas.	9	42,9
Alinear, Planificar, Organizar	01 Gestionar el marco de gestión de TI.	21	100,0
	02 Gestionar la estrategia.	18	85,7
	03 Gestionar la arquitectura empresarial.	18	85, 7
	04 Gestionar la innovación.	19	90,5
	05 Gestionar el portafolio.	13	61,9

CONTINÚA..

	06 Gestionar el presupuesto y los costes.	9	42,9
	07 Gestionar los recursos humanos.	17	81,0
	08 Gestionar las relaciones.	18	85,7
	09 Gestionar los acuerdos de servicio.	13	61,9
	10 Gestionar los proveedores.	15	71,4
	11 Gestionar la calidad.	14	66,7
	12 Gestionar el riesgo.	12	57,1
	13 Gestionar la seguridad.	11	52,4
Construcción, Adquisición e Implementación	01 Gestionar programas y proyectos.	15	71,4
	02 Gestionar la definición de requisitos.	18	85,7
	03 Gestionar la identificación y construcción de soluciones.	11	52,4
	04 Gestionar la disponibilidad y la capacidad.	14	66,7
	05 Gestionar la introducción del cambio organizativo.	13	61,9
	06 Gestionar los cambios.	17	81,0
	07 Gestionar la aceptación del cambio y la transición.	12	57,1
	08 Gestionar el conocimiento.	14	66,7
	09 Gestionar los activos.	8	38,1
	10 Gestionar la configuración.	10	47,6
Entregar, Dar Soporte y Soportado	01 Gestionar operaciones.	16	76,2
	02 Gestionar peticiones e incidentes de servicio.	10	47,6
	03 Gestionar problemas.	17	81,0
	04 Gestionar la continuidad.	18	85,7
	05 Gestionar servicios de seguridad.	12	57,1
	06 Gestionar controles de procesos de negocio.	13	61,9
Supervisión, Evaluación y Verificación	01 Supervisar, evaluar y valorar el rendimiento y la conformidad.	18	85,7
	02 Supervisar, evaluar y valorar el sistema de control interno.	8	38,1
	03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos.	7	33,3

Fuente: Los Autores, (ISACA, 2012)

Con la ayuda de la Tabla 04 donde se encuentra los 39 procesos con sus respectivos valores se genera como resultado la Tabla 05 donde se resumen los dominios y los 17 procesos seleccionados, los mismos que permiten determinar el alcance de la evaluación dentro de la sede.

Tabla 05

Procesos TI seleccionados

PROCESOS COBIT 5

Evaluar, Orientar, Supervisar	01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.
	02 Asegurar la entrega de beneficios.
	04 Asegurar la optimización de recursos.
Alinear, Planificar, Organizar	01 Gestionar el marco de gestión de TI.
	02 Gestionar la estrategia.
	03 Gestionar la arquitectura empresarial.
	04 Gestionar la innovación.
	07 Gestionar los recursos humanos.
	08 Gestionar las relaciones.
	10 Gestionar los proveedores.
Construcción, Adquisición e Implementación	01 Gestionar programas y proyectos.
	02 Gestionar la definición de requisitos.
	06 Gestionar los cambios.
Entrega, Servicio y Soporte	01 Gestionar operaciones.
	03 Gestionar problemas.
	04 Gestionar la continuidad.
Supervisión, Evaluación y Verificación	01 Supervisar, evaluar y valorar el rendimiento y la conformidad.

Fuente: (ISACA, 2012)

Para el establecimiento de los procesos que se evaluarán en la Sede, no es necesario que lo determine únicamente el grupo auditor, se considera adecuado incluir al personal estratégico de la institución que tiene una visión amplia de la naturaleza del negocio y sus necesidades. Se procedió a validar los procesos seleccionados por los auditores con el personal de la institución, estas personas son:

- Teniente Coronel Efrén Cisneros DIRECTOR ESPE - SANTO DOMINGO
- Ing. Eduardo Benavides Docente ESPE - SANTO DOMINGO

Las personas mencionadas determinaron los procesos más importantes de acuerdo a su propio criterio dentro de los 17 procesos ya seleccionados en la Tabla 05 por el grupo auditor. Con la nueva valoración según el nivel de importancia que indica la Tabla 06 se busca delimitar los procesos a evaluar en la ESPE Santo Domingo.

Tabla 06

Criterios para determinar la criticidad de los procesos

PESO	**1**	**2**	**3**	**4**	**5**
CRITERIO	NO ES IMPORTANTE	POCO IMPORTANTE	IMPORTANTE	MUY IMPORTANTE	CRITICO

Fuente: Los Autores

La Tabla 07 muestra la valoración proporcionada por parte del personal de la ESPE Santo Domingo a cada uno de los 17 procesos preseleccionados anteriormente:

Tabla 07

Evaluación de procesos a evaluar

PROCESOS	DESCRIPCIÓN	PREGUNTAS	TCRN. CRNL. AGR. EFRÉN CISNEROS	MG. EDUARDO BENAVIDES
Proceso:	**EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno**			
Descripción**:**	Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las	¿Qué tan importante es este proceso para lograr éxito en la	3	5

CONTINÚA

	responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa	empresa?		
Propósito**:**	Proporcionar un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa. Para garantizar que las decisiones relativas a TI se han adoptado en línea con las estrategias y objetivos de la empresa, garantizando la supervisión de los procesos de manera efectiva y transparentemente, el cumplimiento con los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del Consejo de Administración.			
Proceso:	**EDM02 Asegurar la Entrega de Beneficios**			
Descripción**:**	Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	5
Propósito**:**	Asegurar un valor óptimo de las iniciativas de TI, servicios y activos disponibles; una entrega coste eficiente de los servicios y soluciones y una visión confiable y precisa de los costes y de los beneficios probables de manera que las necesidades del negocio sean soportadas efectiva y eficientemente.			
Proceso:	**EDM04 Asegurar la Optimización de Recursos**			
Descripción**:**	Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	5

CONTINÚA

Propósito**:**	Asegurar que las necesidades de recursos de la empresa son cubiertas de un modo óptimo, que el coste TI es optimizado y que con ello se incrementa la probabilidad de la obtención de beneficios y la preparación para cambios futuros			
Proceso:	**APO01 Gestionar el Marco de Gestión de TI**			
Descripción**:**	Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	5
Propósito**:**	Proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias			
Proceso:	**APO02 Gestionar la Estrategia**			
Descripción**:**	Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	3

CONTINÚA

Propósito**:**	Alinear los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos y las cuentas asociadas para que sean comprendidos por todos, con la identificación de las opciones estratégicas de TI, estructurados e integrados con los planes de negocio.			

Proceso:	**APO03 Gestionar la Arquitectura Empresarial**			
Descripción:	Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información	¿Qué tan importante es este proceso para lograr éxito en la empresa?	2	4
Propósito**:**	Representar a los diferentes módulos que componen la empresa y sus interrelaciones, así como los principios rectores de su diseño y evolución en el tiempo, permitiendo una entrega estándar, sensible y eficiente de los objetivos operativos y estratégicos			

Proceso:	**APO04 Gestionar la Innovación**			
Descripción**:**	Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio.	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	4

CONTINÚA

Propósito**:**	Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa.			
	Lograr ventaja competitiva, innovación empresarial y eficacia y eficiencia operativa mejorada mediante la explotación de los desarrollos tecnológicos para la explotación de la información			
Proceso:	**APO07 Gestionar los Recursos Humanos**			
Descripción**:**	Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	5
Propósito**:**	Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.			
Proceso:	**APO08 Gestionar las Relaciones**			

CONTINÚA

Descripción**:**	Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.	¿Qué tan importante es este proceso para lograr éxito en la empresa?	2	4
Propósito**:**	Crear mejores resultados, mayor confianza en la tecnología y conseguir un uso efectivo de los recursos			
Proceso:	**APO10 Gestionar los Proveedores**			
Descripción**:**	Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.	¿Qué tan importante es este proceso para lograr éxito en la empresa	2	5
Propósito**:**	Minimizar el riesgo de proveedores que no rindan y asegurar precios competitivos.			
Proceso:	**BAI01 Gestión de Programas y Proyectos**			
Descripción**:**	Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia Corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.			

CONTINÚA

Propósito**:**	Alcanzar los beneficios de negocio y reducir el riesgo de retrasos y costes inesperados y el deterioro del valor, mediante la mejora de las comunicaciones y la involucración de usuarios finales y de negocio, asegurando el valor y la calidad de los entregables del proyecto	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	4
Proceso:	**BAI02 Gestionar la Definición de Requisitos**			
Descripción**:**	Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	5
Propósito**:**	Crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan			
Proceso:	**BAI06 Gestionar los Cambios**			
Descripción**:**	Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	3
Propósito**:**	Posibilitar una entrega de los cambios rápida y fiable para el negocio, a la vez que se mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno en que se aplica el cambio.			

CONTINÚA

Proceso:	**DSS01 Gestionar Operaciones**			
Descripción**:**	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	4
Propósito**:**	Entregar los resultados del servicio operativo de TI, según lo planificado.			

Proceso:	**DSS03 Gestionar Problemas**			
Descripción**:**	Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	3
Propósito**:**	Incrementar la disponibilidad, mejorar los niveles de servicio, reducir costes, y mejorar la comodidad y satisfacción del cliente reduciendo el número de problemas operativos			

Proceso:	**DSS04 Gestionar la Continuidad**			
Descripción**:**	Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	5
Propósito**:**	Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.			

CONTINÚA

Proceso:	**MEA01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad**			
Descripción**:**	Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.	¿Qué tan importante es este proceso para lograr éxito en la empresa?	3	3
Propósito**:**	Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.			

Fuente: (ISACA, 2012)

Dependiendo del valor asignado a cada proceso en la Tabla 07, se determinó que los que presentaran los valores más altos serían los seleccionados. En el Anexo 3 y Anexo 4, se puede observar el peso dado por cada una de las personas mencionadas respectivamente.

La Tabla 08 presenta los 10 procesos que serán finalmente evaluados en la ESPE sede Santo Domingo.

Tabla 08

Procesos definitivos a evaluar

PROCESOS COBIT 5	
Evaluar, Orientar, Supervisar	01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.
	02 Asegurar la entrega de beneficios.
	04 Asegurar la optimización de recursos.
Alinear, Planificar, Organizar	01 Gestionar el marco de gestión de TI.
	04 Gestionar la innovación.
	07 Gestionar los recursos humanos.
	10 Gestionar los proveedores.
Construcción, Adquisición e Implementación	01 Gestionar programas y proyectos.
	02 Gestionar la definición de requisitos.
Entrega, Servicio y Soporte	01 Gestionar operaciones.

Fuente: (ISACA, 2012)

3.3.2. Evaluación de los procesos críticos utilizando COBIT 5

Para desarrollar este punto se desplegaron varias actividades, recolección de evidencias por medio de observación directa, visitando la institución, solicitud de documentos de respaldo y entrevistas al personal de la Sede para los cuales evaluamos las actividades que apoyan al cumplimiento del proceso que detalla el documento de COBIT 5.

Las actividades que describe COBIT 5 son las que van a permitir que el proceso se desenvuelva de una manera optimizada y permita alcanzar el objetivo del mismo, estas actividades pueden ser no cumplidas o cumplidas total o parcialmente, solo las actividades que tengan una sustentación por medio de una evidencia podrán ser catalogadas como cumplidas total o parcialmente.

Las personas que ayudaron en el desarrollo de esta parte de la evaluación fueron el Teniente Coronel Efrén Cisneros, DIRECTOR ESPE - Santo Domingo y Mg. Eduardo Benavides, docente ESPE - Santo Domingo

A continuación se presentan en tablas un resumen realizado en base Anexo 5 Plan de Auditoria, que representa cada uno de los 10 procesos evaluados y sus resultados:

Tabla 09

Evaluación Proceso EDM01

PROCESO:	**EDM01 ASEGURAR EL ESTABLECIMIENTO Y MANTENIMIENTO DEL MARCO DE REFERENCIA DE GOBIERNO**
DESCRIPCIÓN:	Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa
PROPÓSITO:	Proporcionar un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa. Para garantizar que las decisiones relativas a TI, se han adoptado en línea con las estrategias y objetivos de la empresa, garantizando la supervisión de los procesos de manera efectiva y transparentemente, el cumplimiento con los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del Consejo de Administración.

	ACTIVIDADES:	**RESPUESTA**	**EVIDENCIA / COMENTARIOS**
1	Analizar e identificar los factores del entorno interno y externo (obligaciones legales, contractuales y regulatorias) y tendencias en el entorno del negocio que pueden influir en el diseño del gobierno.	SI	Diseño de Gobierno corporativo reflejado en el organigrama institucional.
2	Determinar la relevancia de TI y su papel con respecto al negocio.	NO	No existe plan estratégico local, no existe área de TI. (A cargo la UTICs de la Sede Matriz).
3	Considerar las regulaciones externas, obligaciones legales y contractuales y determinar cómo deben ser aplicadas en el gobierno de TI de la empresa.	NO	No existe gobierno de TI, pero las normas que se debe cumplir son: LOES, Norma de control interno, Estatuto de la Universidad, Código de ética.
4	Alinear el uso y el procesamiento ético de la información y su impacto en la sociedad, en el entorno natural y en los intereses de las partes interesadas internas y externas con los objetivos, visión y dirección de la empresa.	NO	El dueño a nivel local Director de la Sede y responsable docente encargado del laboratorio, EL responsable de los sistemas de información es la UTICs en la Sede Matriz.
5	Comprender la cultura empresarial de la toma de decisiones y determinar un modelo óptimo en la toma de decisiones para TI.	NO	No existe unidad de TI, la toma de decisiones la realiza el director de la Sede
6	Comunicar los principios del gobierno de TI y acordar con el gestor ejecutivo la manera de establecer un liderazgo informado y comprometido.	NO	No hay gobierno de TI a nivel de la sede Santo Domingo.

CONTINÚA

7	Establecer o delegar el establecimiento de las estructuras, procesos y prácticas del gobierno en línea con los principios de diseño acordados.	NO	No existe gobierno corporativo de TI.
8	Asignar responsabilidad, autoridad y la responsabilidad de que se apliquen los principios de diseños de gobierno, los modelos de toma de decisión y de delegación acordados.	PARCIALMENTE	La toma de decisiones y responsabilidades se establecen en el organigrama. Los responsables del cumplimiento del diseño corporativo son: EL Director de la sede y el Jefe Administrativo.
9	Garantizar que los mecanismos de notificación y de comunicación proporcionan información adecuada a aquellos con la responsabilidad de la supervisión y toma de decisiones.	PARCIALMENTE	Los mecanismos de comunicación son las publicaciones a través de la web, reunión del personal, email. Pero existen falencias en la comunicación interna debido a que no hay área de TI local.
10	Orientar al personal para que siga las directrices relevantes para un comportamiento ético y profesional y garantizar que las consecuencias del no cumplimiento se conocen y se respetan	SI	Establecidos de forma general en el Código de ética que rige para toda la ESPE.
11	Evaluar la efectividad y rendimiento de las partes interesadas en las que se ha delegado responsabilidad y autoridad para el gobierno de TI de la empresa.	NO	No existen informes de rendimiento, no existe Gobierno de TI.
12	Evaluar periódicamente si los mecanismos para el gobierno de TI acordados (estructuras, principios, procesos, etc.) están establecidos y operando efectivamente.	NO	No existe gobierno de TI.
13	Evaluar la efectividad del diseño del gobierno e identificar las acciones para rectificar cualquier desviación.	NO	No se realizan evaluaciones de la efectividad del diseño de gobierno.
14	Mantener la supervisión sobre el punto hasta el que TI satisface las obligaciones (regulatorias, legislación, leyes comunes, contractuales), políticas internas, estándares y directrices profesionales.	NO	No existe área de TI.
15	Proporcionar supervisión de la efectividad y el cumplimiento, con el sistema de control de la empresa.	PARCIALMENTE	Existe control de acceso físico a las instalaciones de la Sede - Santo Domingo
16	Supervisar los mecanismos rutinarios y regulares para garantizar que el uso de TI cumple con las obligaciones relevantes (regulatorias, legislación, leyes comunes, contractuales), estándares y directrices.	NO	No existe área de TI.

Fuente: Los Autores, (ISACA, 2012)

Tabla 10

Evaluación Proceso EDM02

PROCESO:	**EDM02 ASEGURAR LA ENTREGA DE BENEFICIOS**		
DESCRIPCIÓN:	Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.		
PROPÓSITO:	Asegurar un valor óptimo de las iniciativas de TI, servicios y activos disponibles; una entrega coste eficiente de los servicios y soluciones y una visión confiable y precisa de los costes y de los beneficios probables de manera que las necesidades del negocio sean soportadas efectiva y eficientemente.		
	ACTIVIDADES:	**RESPUESTA**	**EVIDENCIAS / COMENTARIOS**
1	Comprender los requerimientos de las partes interesadas; temas estratégicos de TI, tales como la dependencia de las TI; y comprender la tecnología y sus capacidades considerando la importancia actual y potencial de TI para la estrategia de la empresa.	NO	No existe una dependencia de TI a nivel de la ESPE - Sede Santo Domingo por tanto no hay una estrategia de TI local
2	Comprender los elementos clave de gobierno necesarios para la entrega fiable, segura y coste efectivo de un valor óptimo por el uso de los servicios, activos y recursos de TI existentes y potenciales.	SI	Se tiene conciencia que los servicios de TI locales son clave para alcanzar los objetivos de la Institución.
3	Comprender lo que se entiende por valor en la empresa y considerar cómo de bien se ha comunicado, comprendido y aplicado a través de los procesos de la empresa	SI	Se entiende el concepto de agregar valor a la empresa
4	Evaluar la efectividad de la integración y alineamiento de las estrategias de TI en la empresa y con los objetivos de la empresa para aportar valor.	NO	NO existe estrategia de TI local, hay dependencia de la UTICS de la ESPE Matriz.
5	Comprender y considerar cómo de efectivos son los roles, responsabilidades, asignaciones y organismos de toma de decisiones actuales asegurando la creación de valor de las inversiones, servicios y activos de TI.	NO	Se comprende que la definición de roles y responsabilidades aseguran la creación de valor pero no se tiene documentado
6	Recoger los datos pertinentes, oportunos, completos, fiables y precisos para informar sobre los avances en la entrega de valor respecto a los objetivos.	NO	No se realizan informes de desempeño de TI porque no existe un área de TI local
7	Conseguir informes habituales y relevantes de la cartera, programa y desempeño de TI (tecnológico y funcional). Revisar el progreso de la empresa hacia los objetivos identificados y el grado en el que los objetivos previstos son alcanzados, los entregables obtenidos, los objetivos de rendimiento alcanzados y el riesgo mitigado.	NO	Por lo expuesto anteriormente no se evidencia que se logran los objetivos previstos.

Fuente: Los Autores, (ISACA, 2012)

Tabla 11

Evaluación Proceso EDM04

PROCESO:	**EDM04 ASEGURAR LA OPTIMIZACIÓN DE RECURSOS**		
DESCRIPCIÓN:	Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.		
PROPÓSITO:	Asegurar que las necesidades de recursos de la empresa son cubiertas de un modo óptimo, que el coste TI es optimizado y que con ello se incrementa la probabilidad de la obtención de beneficios y la preparación para cambios futuros		
	ACTIVIDADES:	**RESPUESTA**	**EVIDENCIA / COMENTARIOS**
1	Examinar y evaluar la estrategia actual y futura, las opciones de aprovisionamiento de recursos TI y desarrollar capacidades para cubrir las necesidades actuales y futuras	SI	Se revisa el Inventario de equipos de TI que cubra las necesidades actuales y futura, acordes a la acreditación
2	Definir los principios para guiar la asignación y gestión de recursos y capacidades de manera que las TI pueda satisfacer las necesidades de la empresa, con la habilidad y capacidad requerida	SI	Se tienen asignado de acuerdo a las características de los equipos y a las necesidades de los usuarios.
3	Revisar y aprobar el plan de recursos y las estrategias de arquitectura de la empresa para la entrega de valor y la mitigación de riesgos con los recursos asignados.	NO	No se tienen identificados los riesgos de los programas o recursos de TI
4	Comunicar e impulsar la adopción de estrategias de gestión de recursos, principios y el plan de recursos y las estrategias de arquitectura de la empresa acordada.	NO	No se comunican las estrategias de gestión de recursos
5	Asignar responsabilidades para la ejecución de la gestión de recursos.	SI	El Director de la ESPE - Sede Santo Domingo, Analista de presupuesto y el Docente encargado Mg. Eduardo Benavides, pero no hay área de TI.
6	Definir los objetivos, medidas y métricas clave para la gestión de los recursos.	PARCIALMENTE	Por medio de proyectos y compras públicas
7	Supervisar la asignación y optimización de recursos de acuerdo con los objetivos y prioridades de la empresa mediante objetivos y métricas acordados.	NO	No existen definidas métricas acordadas para la supervisión y asignación de recursos.
8	Supervisar las estrategias de aprovisionamiento TI y de arquitectura de la empresa, los recursos, capacidades de TI para garantizar que las necesidades actuales y futuras de la empresa puedan ser satisfechas.	NO	No se supervisa del aprovisionamiento de TI
9	Supervisar el rendimiento de los recursos frente a los objetivos, analizar las causas de las desviaciones e iniciar acciones correctivas para solucionar las causas subyacentes.	NO	No se supervisan e n base a métricas

Fuente: Los Autores, (ISACA, 2012)

Tabla 12

Evaluación Proceso APO01

PROCESO:	**APO01 GESTIONAR EL MARCO DE GESTIÓN DE TI**		
DESCRIPCIÓN:	Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.		
PROPÓSITO:	Proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias		
	ACTIVIDADES:	**RESPUESTA**	**EVIDENCIA / COMENTARIOS**
1	Definir el alcance, las funciones internas y externas, los roles internos y externos, y las capacidades y los derechos de decisión requeridos, incluidas actividades de TI realizadas por terceras partes	NO	No existe un documento en el cual se detallen las funciones, roles internos y externos, derechos de las actividades realizadas por terceras partes a excepción de lo que indica en los respectivos contratos.
2	Identificar las decisiones necesarias para alcanzar los resultados corporativos y la estrategia de TI y para la gestión y ejecución de servicios de TI	NO	No existe un área de TI en la sede, en consecuencia no existe definido un plan operativo anual, en el que estén definidos los proyectos y servicios de TI para alcanzar los resultados corporativos
3	Establecer la implicación de las partes interesadas críticas para la toma de decisiones (quiénes rendirán cuentas, quiénes son responsables, quiénes deben ser consultados y quiénes informados).	NO	Se conoce la forma jerárquica de trabajo pero no hay documentos formales.
4	Alinear la organización relativa a TI con los modelos organizativos de arquitectura corporativa.	NO	Existe un organigrama de la institución pero no incluye a TI.
5	Definir el enfoque, los roles y las responsabilidades de cada función dentro de la estructura organizativa relativa a TI.	NO	No existe un organigrama establecido para TI
6	Establecer, acordar y comunicar roles y responsabilidades relativos a TI para todo el personal de la empresa, de acuerdo con las necesidades y los objetivos del negocio.	NO	No existe un documento formal de roles y responsabilidades relativos a TI porque no hay un área de TI
7	Incluir en las descripciones de roles y responsabilidades, la adhesión a las políticas y los procedimientos de gestión, al código ético y a las prácticas profesionales.	NO	Existe un código de ética para toda la sede universitaria pero no se incluye en la descripción de los roles y responsabilidades de TI.

CONTINÚA

8	Implementar prácticas de supervisión adecuadas para garantizar que los roles y las responsabilidades se pongan en práctica de forma correcta, para evaluar si todo el personal tiene suficiente autoridad y recursos para llevar a cabo sus roles y responsabilidades, y para hacer una revisión general del rendimiento.	NO	No existen prácticas de supervisión adecuadas que garanticen la práctica adecuada de roles y responsabilidades.
9	Asegurar que la rendición de cuentas queda definida a través de los roles y responsabilidades	NO	No existen documentados la rendición de cuentas de los roles y responsabilidades.
11	Estructurar los roles y responsabilidades para reducir las posibilidades de que un solo rol pueda comprometer un proceso crítico.	NO	No existen Backups para los roles y responsabilidades.
12	Comunicar continuamente los objetivos y la dirección de TI. Asegurar que las comunicaciones reciban apoyo de la dirección ejecutiva, tanto de palabra como mediante acciones, empleando todos los canales disponibles.	NO	No hay una comunicación continua de los objetivos y la dirección de TI.
13	Garantizar que la información comunicada engloba una clara articulación de la misión, los objetivos de servicio, la seguridad, los controles internos, la calidad, el código ético/de conducta, las políticas y procedimientos, los roles y las responsabilidades, etc.	NO	Existen comunicados generales para toda la comunidad universitaria, pero no hay una comunicación a todo nivel de la institución.
14	Proporcionar recursos suficientes y cualificados para dar soporte al proceso comunicativo.	PARCIALMENTE	Existen recursos para la comunicación pero no son los suficientes, ni adecuados.
15	Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información (datos) en toda la empresa	PARCIALMENTE	Existen políticas implementadas a través de la sede matriz.
16	Definir, mantener y proporcionar herramientas adecuadas, técnicas y directrices para garantizar la seguridad y control efectivo sobre la información y los sistemas en colaboración con el propietario	PARCIALMENTE	
17	Crear y mantener un inventario de la información (sistemas y datos) que incluya un listado de los propietarios, custodios y clasificaciones. Incluir los sistemas subcontratados y aquellos cuya propiedad debe permanecer dentro de la empresa.	PARCIALMENTE	
18	Definir e implementar procedimientos para asegurar la integridad y consistencia de toda la información almacenada en formato electrónico, tales como bases de datos, almacenes de datos (data warehouses) y archivos de datos.	NO	A nivel de la sede no existen procedimientos que aseguren la integridad y consistencia de toda la información almacenada en medios electrónicos.
19	Hacer un seguimiento del cumplimiento con políticas y procedimientos	NO	No se revisan, ni realizan informes de cumplimientos porque no existen políticas y procedimientos locales a nivel de TI
20	Analizar los incumplimientos y adoptar las acciones apropiadas (puede incluir el cambio de requerimientos)	NO	No se puede determinar incumplimientos debido a que no existen políticas y procedimientos.

Fuente: Los Autores, (ISACA, 2012)

Tabla 13

Evaluación Proceso APO04

PROCESO:	**APO04 GESTIONAR LA INNOVACIÓN**		
DESCRIPCIÓN:	Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio.		
PROPÓSITO:	Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa.		
	ACTIVIDADES:	**RESPUESTA**	**EVIDENCIA / COMENTARIOS**
1	Crear un plan de innovación que incluya el apetito por el riesgo, el presupuesto previsto para invertir en la innovación y los objetivos de la innovación.	NO	No existe un plan de innovación
2	Proveer de una infraestructura que pueda permitir innovar, tales como herramientas de colaboración para mejorar el trabajo entre diferentes ubicaciones geográficas y divisiones de la empresa.	NO	No existe una infraestructura que permita innovar o mejorar los servicios
3	Realizar reuniones periódicas con las unidades de negocio, divisiones y/o otras entidades interesadas para entender los problemas actuales del negocio, cuellos de botella de los procesos u otras limitaciones donde las tecnologías emergentes o la innovación TI pueden crear oportunidades.	NO	No se realizan reuniones periódicas en las que se consideren tecnologías emergentes o innovación de TI.
4	Valorar la implementación de nuevas tecnologías o innovaciones TI adoptadas como parte de la estrategia TI y desarrollos de la arquitectura empresarial y su realización durante programas de gestión de iniciativas.	NO	No se valora
5	Ajustar el plan de innovación, si fuese necesario.	NO	No hay plan de innovación
6	Identificar y evaluar el posible valor obtenido como fruto del uso de la innovación	NO	No aplica

Fuente: Los Autores, (ISACA, 2012)

Tabla 14

Evaluación Proceso APO10

PROCESO:	**APO10 GESTIONAR LOS PROVEEDORES**		
DESCRIPCIÓN:	Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.		
PROPÓSITO:	Minimizar el riesgo de proveedores que no rindan y asegurar precios competitivos.		
	ACTIVIDADES:	**RESPUESTA**	**EVIDENCIA**
1	Establecer y mantener criterios relativos al tipo, relevancia y criticidad de los contratos y proveedores, focalizándose en aquellos de mayor importancia.	NO	No se dispone de un documento con la Relevancia del contratista y criterios de evaluación
2	Establecer y mantener un criterio de evaluación de contratos y proveedores que permita una revisión general del rendimiento de los proveedores de manera consistente.	NO	No se dispone de un documento con la Relevancia del contratista y criterios de evaluación
3	Identificar, registrar y categorizar los proveedores y contratos existentes de acuerdo al criterio definido para mantener un registro detallado de los proveedores que deben ser gestionados cuidadosamente.	NO	No se dispone de un Catálogo de proveedores
4	Evaluar y comparar periódicamente el rendimiento de los proveedores actuales y alternativos para identificar oportunidades de mejora o la necesidad forzosa de reconsiderar los contratos con los proveedores actuales.	NO	
5	Revisar todas las RFIs y RFPs para asegurar que: •Definen claramente los requisitos. • Incluyen un procedimiento para clarificar los requisitos. •Dan a los proveedores tiempo suficiente para elaborar sus propuestas. •Definen claramente los criterios y el proceso de decisión.	NO	No se encuentran en la sede las RFIs y RFP

CONTINÚA

6	Evaluar RFIs y RFPs de acuerdo al proceso y criterios aprobados y mantener evidencia documental de las evaluaciones. Verificar las referencias de los proveedores candidatos.	NO	No se encuentran en la sede las RFIs y RFP
7	Seleccionar el proveedor que mejor cumpla la RFP. Documentar y comunicar la decisión alcanzada y firmar el contrato.	NO	
8	En el caso específico de la adquisición de software, incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales.	Parcialmente	No se realizan Evaluaciones de RFIs y RFPs
9	En el caso específico de la adquisición de desarrollos, incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales.,	Parcialmente	No se realizan Evaluaciones de RFIs y RFPs
11	En el caso específico de la adquisición de infraestructuras, instalaciones y servicios relacionados, incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales.	Parcialmente	No se realizan Evaluaciones de RFIs y RFPs
12	Asignar propietarios de la relaciones para cada proveedor y hacerles responsables de la calidad del servicio proporcionado.	NO	No se designa Roles y responsabilidades de los proveedores
14	Acordar, gestionar, mantener y renovar los contratos con los proveedores. Asegurar que los contratos son conformes con las normas corporativas y con los requisitos legales y regulatorios.	Parcialmente	Los contratos no se encuentran en la sede
15	Incluir en los contratos con los proveedores de servicios clave disposiciones para revisar los lugares de trabajo y las prácticas y controles de la dirección o de terceras partes.	NO	
16	Definir y formalizar los roles y responsabilidades de cada proveedor. Cuando varios proveedores se combinan para proporcionar un servicio, considerar asignar un rol de proveedor líder a uno de los proveedores para que asuma la responsabilidad global del contrato.	NO	

CONTINÚA

17	A la hora de definir el contrato, para los riesgos potenciales, incluir una descripción clara de todos los requisitos de servicio, incluyendo depósitos de garantía, proveedores alternativos o acuerdos en suspenso para mitigar el riesgo de un posible fallo del proveedor; los aspectos de seguridad, la propiedad intelectual y los requisitos legales y regulatorios	NO	
18	Supervisar y revisar la entrega de servicios para asegurar que el proveedor está proporcionando una calidad del servicio adecuada, cumpliendo los requisitos y las condiciones de los contratos.	NO	No se supervisa el cumplimiento de los proveedores
19	Revisar el rendimiento y el coste de los proveedores para asegurar que son competitivos y fiables, en comparación con proveedores alternativos y condiciones de mercado.	NO	No se supervisa el cumplimiento de los proveedores
20	Solicitar revisiones independientes de las prácticas internas y los controles, si se considera necesario.	NO	No se supervisa el cumplimiento de los proveedores
21	Registrar y evaluar los resultados de la revisión periódica y discutirlos con el proveedor para identificar las necesidades y oportunidades de mejora.	NO	No se supervisa el cumplimiento de los proveedores
22	Supervisar y evaluar la información externa disponible sobre el proveedor.	NO	No se supervisa el cumplimiento de los proveedores

Fuente: Los Autores, (ISACA, 2012)

Tabla 15

Evaluación Proceso BAI01

PROCESO:	**BAI01 GESTIÓN DE PROGRAMAS Y PROYECTOS**		
DESCRIPCIÓN:	Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia Corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.		
PROPÓSITO:	Alcanzar los beneficios de negocio y reducir el riesgo de retrasos y costes inesperados y el deterioro del valor, mediante la mejora de las comunicaciones y la involucración de usuarios finales y de negocio, asegurando el valor y la calidad de los entregables del proyecto y maximizando su contribución al portafolio de servicios e inversiones.		
	ACTIVIDADES:	**RESPUESTA**	**EVIDENCIA**
1	Mantener y reforzar un enfoque estándar de la gestión de programas y proyectos alineados al entorno específico de la empresa, y a las buenas prácticas basadas en procesos definidos y el uso de tecnología apropiada.	NO	La sede no cuenta con un plan de gestión de programas y proyectos
2	Actualizar el enfoque de gestión de programas y proyectos sobre la base de las lecciones aprendidas en su uso.	NO	La sede no cuenta con un plan de gestión de programas y proyectos
3	Acordar el patrocinio del programa y designar una Junta/Comité con miembros que tengan intereses estratégicos en el programa y con responsabilidad en la toma de decisiones de inversión, que serán afectados significativamente por el programa y que serán necesarios para facilitar el cambio.	NO	No se designa un comité para los programas que tomen decisiones de inversión
4	Confirmar el mandato del programa con los patrocinadores y las partes interesadas. Articular los objetivos estratégicos para el programa, las estrategias potenciales de entrega, las mejoras y los beneficios que se esperan y cómo el programa encaja con otras iniciativas.	NO	No existe el caso de negocio de concepto del programa

CONTINÚA

5	Desarrollar un caso de negocio detallado para el programa, si se justifica. Involucrar a todas las partes interesadas relevantes para desarrollar y documentar un entendimiento completo de los resultados esperados por la empresa,	NO	No existe el caso de negocio de concepto del programa
6	Desarrollar un plan de realización de beneficios que será gestionado durante todo el programa para asegurar que los beneficios planificados siempre tengan propietarios, se logren, sostengan y optimicen.	NO	
7	Preparar y someter a aprobación preliminar el caso de negocio inicial (conceptual) del programa, proporcionando información esencial para la toma de decisiones respecto del propósito, la contribución a los objetivos del negocio, la creación de valor esperado, los márgenes de tiempo, etc.	NO	No existe el caso de negocio de concepto del programa
8	Designar un gerente dedicado para el programa, con las competencias y habilidades adecuadas para gestionar el programa de forma eficiente y efectiva	NO	Existe poco personal
9	Planificar la forma en que las partes interesadas internas y externas de la empresa serán identificadas, analizadas, comprometidas, y gestionadas a lo largo del ciclo de vida de los proyectos.	NO	No existe un plan que involucre a las partes interesadas
10	Identificar, comprometer y gestionar a las partes interesadas, estableciendo y manteniendo niveles apropiados de coordinación, comunicación y vinculación para asegurar que estén involucrados en los programas/proyectos.	NO	No existe un plan que involucre a las partes interesadas
11	Medir la efectividad del compromiso de las partes interesadas y tomar acciones de remediación si es necesario.	NO	No existe un plan que involucre a las partes interesadas
12	Analizar los intereses y los requisitos de las partes interesadas.	NO	No existe un plan que involucre a las partes interesadas
13	Definir y documentar el plan de programa cubriendo todos los proyectos, incluyendo lo que sea necesario para lograr cambios en la empresa; su imagen, productos y servicios, procesos de negocio, habilidades y cantidad de personal, requerimientos tecnológicos, relaciones con las partes interesadas, clientes, proveedores, entre otros,	NO	No existe un Plan de programa

CONTINÚA

14	Especificar las habilidades y los recursos necesarios para ejecutar el proyecto, incluyendo los gerentes y los equipos del proyecto, así como los recursos del negocio. Especificar la financiación, coste, cronograma y las interdependencias de los múltiples proyectos.	NO	No existe un Presupuesto del programa y registro de beneficios
15	Asignar la responsabilidad ejecutiva para cada proyecto en forma clara y sin ambigüedades, incluyendo el logro de los beneficios, el control de costes, la gestión de riesgos y la coordinación de las actividades de los proyectos.	NO	No se redactan los Requerimientos de recursos y roles
16	Asegurar que existe una comunicación efectiva de los planes de programa e informes de avance sobre todos los proyectos y con todo el programa. Asegurar que cualquier cambio hecho en los planes individuales se refleje en el resto de planes de programa de la empresa.	NO	No existe un Plan de programa
17	Actualizar y mantener el caso de negocio y el registro de beneficios a lo largo de la vida económica del programa para identificar y definir los beneficios principales surgidos de los programas ejecutados.	NO	No existe el caso de negocio de concepto del programa
18	Preparar un presupuesto del programa que refleje los costes del ciclo de vida económica completa, así como los beneficios financieros y no financieros asociados.	NO	No existe un Presupuesto del programa y registro de beneficios
19	Establecer etapas acordadas para el proceso de desarrollo (puntos de verificación del desarrollo). Al final de cada etapa, facilitar discusiones formales de los criterios aprobados con las partes interesadas.	NO	No existe una supervisión del logro de metas del programa
20	Llevar a cabo un proceso de obtención de beneficios durante el programa para asegurar que los beneficios planeados siempre tienen propietarios y que es probable que se consigan, mantengan y se optimicen.	NO	No existe una supervisión del logro de metas del programa
21	Establecer oficina(s) de gestión de programas/proyectos y planificar auditorías, revisiones de calidad, revisiones de cambios de fase (stage-gate), y revisiones de los beneficios realizados.	NO	No se planifican Planes de auditoría del programa

Fuente: Los Autores, (ISACA, 2012)

Tabla 16

Evaluación Proceso BAI02

PROCESO:	**BAI02 GESTIONAR LA DEFINICIÓN DE REQUISITOS**		
DESCRIPCIÓN:	Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.		
PROPÓSITO:	Crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan		
	ACTIVIDADES:	**RESPUESTA**	**EVIDENCIA**
1	Definir e implementar la definición de requerimientos y el procedimiento de mantenimiento y un repositorio de requisitos acorde al tamaño, complejidad, objetivos y riesgos de la iniciativa que la empresa está considerando acometer.	NO	No existe un repositorio de definición de requerimientos
2	Expresar los requerimientos de la empresa en términos de cómo la diferencia entre las capacidades del negocio existente y deseadas son tratadas y como cada rol interactuará con la solución y la utilizará.	NO	No existe un repositorio de definición de requerimientos
3	Durante todo el proyecto, obtener, analizar y confirmar que los requerimientos de todas las partes interesadas, incluyendo los criterios de aceptación relevantes, son considerados, obtenidos, priorizados y registrados de un modo comprensible para las partes interesadas, patrocinadores de negocio y personal de la implementación técnica	NO	No existe un repositorio de definición de requerimientos
4	Especificar y priorizar la información, los requerimientos técnicos y funcionales basados en los requerimientos de las partes interesadas. Incluir requerimientos de control de la información en los procesos de negocio, procesos automatizados y entornos de TI para hacer frente a los riesgos de la información y cumplimiento con regulaciones, leyes y contratos comerciales.	NO	No existe un repositorio de definición de requerimientos

CONTINÚA

5	Validar todos los requerimientos mediante aproximaciones tales como revisión por iguales, validación del modelo o prototipo operativo.	NO	No existe un repositorio de definición de requerimientos
6	Confirmar la aceptación de aspectos clave de los requerimientos, incluyendo reglas de negocio, controles de información, continuidad de negocio, cumplimiento legal y regulatorio, 'audibilidad', ergonomía, operatividad y usabilidad, seguridad y soporte documental.	NO	No existe un repositorio de definición de requerimientos
7	Definir y ejecutar un estudio de viabilidad, piloto o solución básica funcional que clara y concisamente describa las soluciones alternativas que satisfarán los requerimientos funcionales y de negocio. Incluir una evaluación de su viabilidad técnica y económica.	NO	No existe un informe de estudio de viabilidad
8	Identificar las acciones requeridas para la adquisición o desarrollo de la solución, basada en la arquitectura de la empresa y tener en cuenta el alcance y/o tiempo y/o limitaciones de presupuesto.	NO	No poseen un Plan de alto nivel de adquisiciones/desarrollo
9	Revisar las soluciones alternativas con todas las partes interesadas y seleccionar la más apropiada basada en criterios de viabilidad, incluyendo costes y riesgos.	NO	No se posee un catálogo de proveedores
10	Traducir la línea de acción preferida a un plan de alto de nivel de adquisición/desarrollo identificando recursos a utilizar y fases que requieran decisiones de continuar/no continuar.	NO	No poseen un Plan de alto nivel de adquisiciones/desarrollo
11	Involucrar a las partes interesadas para crear una lista potencial de requerimientos técnicos, funcionales, de calidad y riesgos relativos al procesamiento de la información	NO	No existe un repositorio de definición de requerimientos
12	Analizar y priorizar los riesgos de los requerimientos conforme probabilidad e impacto. Si aplica, determinar los impactos en coste y tiempo.	NO	No existe un análisis de riesgos de los requerimientos
13	Identificar modos de controlar, evitar o mitigar los riesgos de los requerimientos en orden de prioridad	NO	
14	Obtener revisiones de calidad completas y de cada fase clave del proyecto, iteración o versión comparando los resultados obtenidos contra los criterios originales de aceptación. Disponer de la firma del patrocinador y otros interesados en cada revisión de calidad.	NO	No tiene un plan de gestión de la calidad

Fuente: Los Autores, (ISACA, 2012)

Tabla 17

Evaluación Proceso DSS01

PROCESO:	**DSS01 GESTIONAR OPERACIONES**		
DESCRIPCIÓN:	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.		
PROPÓSITO:	Entregar los resultados del servicio operativo de TI, según lo planificado.		
	ACTIVIDADES:	**RESPUESTA**	**EVIDENCIA**
1	Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados.	Parcialmente	No existe suficiente personal
2	Mantener una programación de actividades operativas, ejecutar las actividades y gestionar el desempeño y rendimiento (throughput) de las actividades programadas.	NO	No existe una programación operativa
3	Asegurar que se cumple con los estándares de seguridad aplicables para la recepción, procesamiento, almacenamiento y salida de datos de forma tal que se satisfagan los objetivos empresariales, la política de seguridad de la empresa y los requerimientos regulatorios.	Parcialmente	Utilizan ciertos estándares
4	Verificar que todos los datos esperados para su procesamiento sean recibidos y procesados por completo y de una forma precisa y oportuna. Entregar los resultados de acuerdo con los requisitos de la empresa. Dar soporte a las necesidades de reinicio y reprocesamiento	NO	No existe un registro de los servicios brindados en la sede
5	Asegurar que los procesos de información se adhieren a los requerimientos de seguridad de la empresa y conformes con los contratos y ANSs con terceros que alojan o proveen servicios.	NO	No se tiene definido los OLAs

CONTINÚA

7	Integrar los procesos críticos de gestión interna de TI con los de los proveedores de servicios externalizados cubriendo, por ejemplo, la planificación de la capacidad y el rendimiento, la gestión del cambio, la gestión de la configuración, la gestión de peticiones de servicio y de incidentes, gestión de problemas, la gestión de la seguridad.	NO	No se definen los SLAs de los servicios
8	Registrar eventos, identificando el nivel de información a ser grabada sobre la base de una consideración del riesgo y el rendimiento.	NO	No existe un registro de eventos
9	Identificar y mantener una lista de activos de infraestructura que necesiten ser monitorizados en base a la criticidad del servicio y la relación entre los elementos de configuración y los servicios que de ellos dependen.	Parcialmente	Disponen de ciertos equipos
10	Definir e implantar reglas que identifiquen y registren violaciones de umbral y condiciones de eventos. Encontrar un equilibrio entre la generación de eventos falsos menores y eventos significativos	NO	No se establecen reglas de monitorización de activos y condiciones de eventos
11	Producir registros de eventos y retenerlos por un periodo apropiado para asistir en investigaciones futuras.	NO	No existe un registro de eventos
12	Establecer procedimientos para supervisar los registros de eventos y llevar a cabo revisiones periódicas.	NO	No existe un registro de eventos
13	Identificar desastres naturales y causados por el ser humano que puedan ocurrir en el área donde se encuentran las instalaciones de TI. Evaluar el efecto potencial en las instalaciones de TI.	NO	
14	Ubicar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad ante las amenazas del entorno.	NO	No se analizó la ubicación de las instalaciones de TI
15	Supervisar y mantener de forma periódica a los dispositivos que detectan proactivamente las amenazas del entorno (p. ej. fuego, agua, humo, humedad).	Parcialmente	

CONTINÚA

16	Examinar los requerimientos de las instalaciones de TI respecto de la protección frente a la fluctuación y cortes de la energía eléctrica, en relación con otros requerimientos de la planificación de la continuidad del negocio.	NO	No existe el análisis
17	Disponer de equipamiento adecuado de alimentación ininterrumpida (p. ej. baterías, generadores) para dar soporte a la planificación de continuidad del negocio.	NO	
18	Probar periódicamente los mecanismos del sistema de alimentación ininterrumpida (SAI) y asegurar que la electricidad puede ser conmutada al sistema sin efectos significativos en las operaciones del negocio.	NO	No existe los SAI
19	Asegurar que las instalaciones que alojan los sistemas de TI tienen más de un proveedor para los servicios públicos indispensables (p. ej. electricidad, telecomunicaciones, agua, gas). Separar la acometida de cada servicio.	NO	Solo se tiene un proveedor
20	Confirmar que el cableado externo al sitio TI está bajo tierra o que tiene una protección alternativa adecuada. Determinar que el cableado en el sitio TI está contenido en conductos asegurados y que los armarios de cableado tienen su acceso restringido al personal autorizado.	Parcialmente	Por medio de una ficha de observación se comprobó
21	Asegurar que el cableado y el patching físico (datos y telefonía) están estructurados y organizados. Las estructuras de cableado y de conductos debieran estar documentadas (p.ej. plano del edificio y diagramas de cableado).	NO	
22	Asegurar que los sitios e instalaciones de TI cumplen de manera sistemática con la legislación, regulaciones, directrices y especificaciones relevantes de salud y seguridad en el trabajo.	SI	Por medio de una ficha de observación se comprobó

Fuente: Los Autores, (ISACA, 2012)

3.3.3. Evaluación de madurez de los procesos críticos utilizando COBIT 5

El siguiente paso del trabajo es determinar la madurez de los procesos mediante el documento de COBIT 5 "Self Assessment Guide Using Cobit 5" que es una metodología concisa, fiable y robusta para evaluar la capacidad de sus procesos de TI proporcionada para las empresas. Dentro de esta guía, la madurez se expresa en una escala que va desde el 0 al 5 como lo podemos ver en la siguiente tabla:

Tabla 18

Medición de Madurez

MEDICIÓN DE MADUREZ DEL PROCESO	
NIVEL DEL PROCESO	**MADUREZ**
Nivel 0 (Incompleto)	El proceso no se ha implementado, o no ha logrado conseguir su propósito
Nivel 1 (Ejecutado)	El proceso alcanza su propósito.
Nivel 2 (Gestionado)	El proceso esta implementado y gestionado (planificado, monitoreado y ajustado) y sus productos están adecuadamente establecidos, controlados y mantenidos.
Nivel 3 (Establecido)	El proceso esta implementado y se usa un proceso definido que permite obtener los resultados deseados.
Nivel 4 (Predecible)	El proceso opera dentro de los límites establecidos y alcanza resultados deseados.
Nivel 5 (Optimizado)	El proceso es predecible y se mejora continuamente para contribuir con las metas del negocio.

Fuente: (ISACA, 2012)

Para determinar el nivel de madurez del proceso se realiza una cuantificación a las evidencias de cada proceso en función de la siguiente tabla que nos brinda la guía "Self Assessment guide Using Cobit 5" la escala calificación son un estándar definido en la norma ISO / IEC 15504.

Tabla 19

Niveles de Medición

NIVELES DE MEDICIÓN		
N	No se alcanzo	0 al 15%
P	Se alcanzó parcialmente	>15% al 50%
L	Alcanzado en gran medida	> 50% al 85%
F	Totalmente alcanzado	>85% al 100%

Fuente: (ISACA, 2012)

A continuación se presentan las matrices de análisis del estado de madurez de los procesos seleccionados referidas en el documento Self Assessment Templates de COBIT 5:

Tabla 20

Calificación proceso EDM01

Proceso	Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
EDM01		PA 1.1	PA 2.1 PA 2.2	PA 3.1 PA 3.2	PA 4.1 PA 4.2	PA 5.1 PA5.2
Puntuación de los criterios		P (15%)				
Nivel de Madurez Conseguido	0					
			N (0-15%)	**P(15% - 50%)**	**L(50% - 85%)**	**F (85% - 100%)**

Fuente: Los Autores

Tabla 21

Madurez proceso EDM01

PROCESO:	**EDM01 ASEGURAR EL ESTABLECIMIENTO Y MANTENIMIENTO DEL MARCO DE REFERENCIA DE GOBIERNO**
DESCRIPCIÓN:	Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa
PROPÓSITO:	Proporcionar un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa. Para garantizar que las decisiones relativas a TI se han adoptado en línea con las estrategias y objetivos de la empresa, garantizando la supervisión de los procesos de manera efectiva y transparentemente, el cumplimiento con los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del Consejo de Administración

CONTINÚA

EDM01	Evaluar si se consiguen los siguientes resultados	Criterios	Cumple con los Criterios S/N	Comentarios	No Alcanzados (0-15%)	Parcialmente Alcanzados (15% - 50%)	Alcanzado en Gran Medida (50% - 85%)	Totalmente Alcanzado (85% - 100%)
Nivel 0 Incompleto	El proceso no se ha implementado, o no ha logrado conseguir su propósito	En este nivel, hay pocas o ninguna evidencia del cumplimiento del propósito del proceso						
Nivel 1 Ejecutado	PA1.1 El proceso alcanza su propósito	Los siguientes resultados del proceso se están cumpliendo						
		Modelo estratégico de toma de decisiones para que las TI sean efectivas y estén alineadas con el entorno externo e interno de la empresa y los requerimientos de las partes interesadas.	SI	Se lo puede observar en el organigrama institucional		35%		
		Garantizar que el sistema de gobierno para TI está incorporado al gobierno corporativo.	NO					
		Obtener garantías de que el sistema de gobierno para TI está operando de manera efectiva.	NO					

CONTINÚA

Nivel 2 Gestionado	PA 2.1 Gestión del desempeño- Una medida dl grado en que se gestiona el desempeño del proceso	Como resultado de la plena consecuencia de este atributo:	
		a. Los objetivos de desempeño del proceso son identificados	
		b. El desempeño del proceso está planeado y monitoreado	
		c. El desempeño del proceso está ajustado para cumplir los planes	
		d. Los responsables y las autoridades encargados del proceso están definidos asignados y comunicados	
		e. Los recursos e información necesaria para ejecutar el proceso están identificados, disponibles, asignados y utilizados.	
		f. Las interfaces entre las partes interesadas son gestionadas para garantizar una comunicación efectiva y una clara asignación de responsabilidades	
	PA 2.2 Gestión del producto del trabajo- Una medida del grado en la	Como resultado de la plena consecuencia de este atributo:	
		a. Los requerimientos para los productos de trabajo del proceso están definidos.	

CONTINÚA

	que los productos de trabajo proporcionados por el proceso son bien manejados, Los productos de trabajo (o salida del proceso) se definen y controlan.	b. Los requisitos de documentación y control del producto de trabajo están definidos.	
		c. Los productos de trabajo están adecuados, identificados, adecuados, documentados y controlados	
		d. Los productos de trabajo son revisados de acuerdo a un plan previsto y ajustados si es necesario para cumplir con los requerimientos.	
Nivel 3 Establecido	PA 3.1 Definición del proceso .- Una medida del grado en que mantiene un proceso estándar para apoyar el desarrollo de un proceso definido	Como resultado de la plena consecuencia de este atributo:	
		a. Un proceso estándar incluyendo guías de adaptación adecuadas, se definen para describir los principales fundamentos que deben ser incorporados en un proceso determinado	
		b. La secuencia e interacción de un proceso estándar con otros procesos está determinado.	
		c. Las competencias requeridas y los roles para ejecutar un proceso están definidas como parte de un	

CONTINÚA

	proceso estándar.	
	d. La infraestructura requerida y el ambiente de trabajo para ejecutar un proceso están definidas como parte de un proceso estándar.	
	e. Métodos de trabajo adecuados para monitorear la efectividad y ajuste del proceso están definidos.	
PA3.2 Desarrollo del proceso Una medida del grado en que un proceso estándar es efectivamente desplegado como un proceso definido para lograr sus resultados	Como resultado de la plena consecuencia de este atributo:	
	a. Un proceso definido se implementa en base a un proceso estándar debidamente seleccionado o adaptado	
	b. Los roles, responsabilidades y autoridades requeridas para ejecutar un proceso están asignados y comunicados.	
	c. El personal que ejecuta el proceso es competente; tiene una educación, entrenamiento y experiencia apropiados.	

CONTINÚA

		d. Los recursos e información necesaria para ejecutar un proceso definido están disponibles, asignados y utilizados	
		e. La infraestructura y ambiente de trabajo requeridos para ejecutar un proceso definido disponibles, gestionados conservados.	
		f. Los datos apropiados recolectados y analizados para entender su comportamiento, además para demostrar la idoneidad efectividad del proceso así como para evaluar donde se puede aplicar un mejoramiento continuo.	
Nivel 4 Predecible	PA 4.1 Medición de Proceso - Una medida del grado en que los resultados de una medición se utilizan para asegurar que el rendimiento	Como resultado de la plena consecuencia de este atributo:	
		a. Están establecidas las medidas de información del proceso para apoyar las metas de la empresa	
		b. Los objetivos de medición del proceso se derivan de las necesidades de información del proceso para apoyar las metas de la empresa	

CONTINÚA

	del proceso apoya el logro de los objetivos de las metas del negocio	c. Los objetivos cuantitativos para el desempeño del proceso que apoyan las metas relevantes de la empresa están establecidos.	
		d. Las medidas y la frecuencia de la medición están identificadas y definidas en función de los objetivos de medida del proceso y de los objetivos cuantitativos de desempeño del mismo	
		e. Los resultados de la medición son recolectados, analizados y reportados para monitorear el grado en el que los objetivos de desempeño del proceso se cumplen.	
		f. Los resultados de la medición son utilizados para determinar el desempeño del proceso.	
	PA 4.2 Control del proceso - Una medida del grado en el que el proceso es gestionado cuantitativamente para	Como resultado de la plena consecuencia de este atributo:	
		a. Técnicas de control y análisis están determinadas y aplicadas donde es posible	
		b. Los límites de control de variación están establecidos para el desempeño normal del proceso	

CONTINÚA

	conseguir un proceso estable, competente y predecible dentro de los límites definidos.	c. Se analizan datos de medición cuando hay causas especiales de variación.	
		d. Se toman acciones correctivas para afrontar las causas especiales de variación.	
		e. Los límites de control son reestablecidos (cuando es necesario) después de una acción correctiva.	
Nivel 5 Optimizado	PA 5.1 Innovación del proceso - Una medida del grado en que los cambios en el proceso son identificados a partir de una análisis de caudas comunes de variación en el rendimiento	Como resultado de la plena consecuencia de este atributo:	
		a. Los objetivos de mejora del proceso que apoyan las metas relevantes de la empresa están definidos	
		b. Datos apropiados son analizados para identificar las causa comunes de las variaciones en el rendimiento del proceso	
		c. Datos apropiados son analizados para identificar las causa comunes de las variaciones en el rendimiento del proceso	
		d. .Datos apropiados son analizados para identificar oportunidades de aplicar mejores	

CONTINÚA

		prácticas innovación.	
		e. Oportunidades de mejora derivadas de nuevas tecnologías y conceptos de proceso están identificadas.	
		f. Una estrategia de implementación está establecida para conseguir los objetivos de mejora del proceso.	
	PA5, 2 Optimización del proceso - Una medida del grado en que los cambios en la definición gestión y rendimiento del resultado del proceso en impacto efectivo logra sus objetivos de mejora.	Como resultado de la plena consecuencia de este atributo:	
		a. El impacto de los cambios propuestos se evalúan en función de los objetivos del proceso definido y del estándar	
		b. Se gestiona la implementación de todos los cambios aceptados para asegurar el entendimiento y acción sobre cualquier interrupción en el funcionamiento del proceso.	Madures
		c. En base al desempeño actual, la efectividad del cambio en el proceso se evalúa en función de la definición de los requerimientos del producto	

Fuente: Los Autores, (ISACA, 2012)

Tabla 22

Calificación proceso EDM02

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	NIVEL 5
EDM02		PA 1.1	PA 2.1 PA 2.2	PA 3.1 PA 3.2	PA 4.1 PA 4.2	PA 5.1 PA5.2
Puntuación de los criterios		P (13%)				
Nivel de Madurez Conseguido	0					
			N (0-15%)	**P(15% - 50%)**	**L(50% - 85%)**	**F (85% - 100%)**

Fuente: Los Autores, (ISACA, 2012)

Tabla 23

Madurez proceso EDM02

PROCESO:	**EDM02 ASEGURAR LA ENTREGA DE BENEFICIOS**							
DESCRIPCIÓN:	Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.							
PROPÓSITO:	Asegurar un valor óptimo de las iniciativas de TI, servicios y activos disponibles; una entrega coste eficiente de los servicios y soluciones y una visión confiable y precisa de los costes y de los beneficios probables de manera que las necesidades del negocio sean soportadas efectiva y eficientemente.							
EDM02	**Evaluar si se consiguen los siguientes resultados**	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	**No Alcanzados (0-15%)**	**Parcialmente Alcanzados (15% - 50%)**	**Alcanzado en Gran Medida(50% -85%)**	**Totalmente Alcanzado (85% - 100%)**
Nivel 0 Incompleto	El proceso no se ha implementado , o no ha logrado conseguir su propósito	En este nivel, hay pocas o ninguna evidencia del cumplimiento del propósito del proceso						
Nivel 1 Ejecutado	PA1.1 El proceso alcanza su propósito	Los siguientes resultados del proceso se están cumpliendo						
		La empresa está asegurando un valor óptimo de su portafolio de iniciativas TI, servicios y activos aprobados.	Si	Si tienen conciencia de la importancia de los servicios que TI		40%		

CONTINÚA

	presta	
	Se deriva un valor óptimo de la inversión TI mediante prácticas de gestión del valor en la empresa.	No
	Las inversiones individuales en TI contribuyen a un valor óptimo.	No

Fuente: Los Autores, (ISACA, 2012)

Tabla 24

Calificación proceso EDM04

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	NIVEL 5
EDM04		PA 1.1	PA 2.1 PA 2.2	PA 3.1 PA 3.2	PA 4.1 PA 4.2	PA 5.1 PA5.2
Puntuación de los criterios		P (30%)				
Nivel de Madurez Conseguido	0					
			N (0-15%)	**P(15% - 50%)**	**L (50% - 85%)**	**F (85% - 100%)**

Fuente: Los Autores, (ISACA, 2012)

Tabla 25

Madurez proceso EDM04

PROCESO:	**EDM04 ASEGURAR LA OPTIMIZACIÓN DE RECURSOS**							
DESCRIPCIÓN:	Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.							
PROPÓSITO:	Asegurar que las necesidades de recursos de la empresa son cubiertas de un modo óptimo, que el coste TI es optimizado y que con ello se incrementa la probabilidad de la obtención de beneficios y la preparación para cambios futuros							
EDM04	**Evaluar si se consiguen los siguientes resultados**	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	**No Alcanzados (0-15%)**	**Parcialmente Alcanzados (15% - 50%)**	**Alcanzado en Gran Medida (50% - 85%)**	**Totalmente Alcanzado (85% -100%)**
Nivel 0 Incompleto	El proceso no se ha implementado, o no ha logrado conseguir su propósito	En este nivel, hay pocas o ninguna evidencia del cumplimiento del propósito del proceso						
Nivel 1 Ejecutado	PA1.1 El proceso alcanza su propósito	Los siguientes resultados del proceso se están cumpliendo						
		Las necesidades de recursos de la empresa son cubiertas con capacidades óptimas.	Si	Las necesidades de la		40%		

CONTINÚA

		empresa son cubiertas parcialmente	
	Los recursos se asignan para satisfacer mejor las prioridades de la empresa dentro del presupuesto y restricciones...	Si	30%
	El uso óptimo de los recursos se logra a lo largo de su completo ciclo de vida económico.	Si	20%

Fuente: Los Autores, (ISACA, 2012)

Tabla 26

Calificación proceso APO01

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	NIVEL 5
APO01		PA 1.1	PA 2.1 PA 2.2	PA 3.1 PA 3.2	PA 4.1 PA 4.2	PA 5.1 PA5.2
Puntuación de los criterios		P (20%)				
Nivel de Madurez Conseguido	0					
			N (0-15%)	**P (15% - 50%)**	**L (50% - 85%)**	**F (85% - 100%)**

Fuente: Los Autores, (ISACA, 2012)

Tabla 27

Madurez proceso APO01

PROCESO:	**APO01 GESTIONAR EL MARCO DE GESTIÓN DE TI**							
DESCRIPCIÓN:	Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.							
PROPÓSITO:	Proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias							
APO01	**Evaluar si se consiguen los siguientes resultados**	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	**No Alcanzados (0-15%)**	**Parcialmente Alcanzados (15% - 50%)**	**Alcanzado en Gran Medida (50% -85%)**	**Totalmente Alcanzado (85% -100%)**
Nivel 0 Incompleto	El proceso no se ha implementado , o no ha logrado conseguir su propósito	En este nivel, hay pocas o ninguna evidencia del cumplimiento del propósito del proceso						
Nivel 1 Ejecutado	PA1.1 El proceso alcanza su propósito	Los siguientes resultados del proceso se están cumpliendo						
		Se ha definido y se mantiene un conjunto eficaz de políticas.	No					

CONTINÚA

	Todos tienen conocimiento de las políticas y de cómo deberían implementarse.	Si	No todas las personas tiene conocimiento de las políticas	40%

Fuente: Los Autores, (ISACA, 2012)

Tabla 28

Calificación proceso APO04

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	NIVEL 5
APO04		PA 1.1	PA 2.1 PA 2.2	PA 3.1 PA 3.2	PA 4.1 PA 4.2	PA 5.1 PA5.2
Puntuación de los criterios						
Nivel de Madurez Conseguido	0					
			N (0-15%)	**P (15% -50%)**	**L (50% -85%)**	**F (85% -100%)**

Fuente: Los Autores, (ISACA, 2012)

Tabla 29

Madurez proceso APO04

PROCESO:	**APO04 GESTIONAR LA INNOVACIÓN**							
DESCRIPCIÓN:	Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio.							
PROPÓSITO:	Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa.							
APO04	**Evaluar si se consiguen los siguientes resultados**	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	**No Alcanzados (0-15%)**	**Parcialmente Alcanzados (15% - 50%)**	**Alcanzado en Gran Medida (50% - 85%)**	**Totalmente Alcanzado (85% - 100%)**
Nivel 0 Incompleto	El proceso no se ha implementado , o no ha logrado conseguir su propósito	En este nivel, hay pocas o ninguna evidencia del cumplimiento del propósito del proceso						
Nivel 1 Ejecutado	PA1.1 El proceso alcanza su propósito	Los siguientes resultados del proceso se están cumpliendo						
		El valor de empresa es creado mediante la cualificación y puesta en escena de los avances e innovaciones tecnológicas más apropiadas,	No					

CONTINÚA

	los métodos y las soluciones TI utilizadas	
	Los objetivos de la empresa se cumplen por la mejora de los beneficios de la calidad y/o la reducción de costes como resultado de la identificación e implementación de soluciones innovadoras.	No
	La innovación se permite y se promueve y forma parte de la cultura de la empresa.	No

Fuente: Los Autores, (ISACA, 2012)

Tabla 30

Calificación proceso APO07

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	NIVEL 5
APO07		PA 1.1	PA 2.1 PA 2.2	PA 3.1 PA 3.2	PA 4.1 PA 4.2	PA 5.1 PA5.2
Puntuación de los criterios		P (25%)				
Nivel de Madurez Conseguido	0					
			N (0-15%)	**P (15% -50%)**	**L (50% -85%)**	**F (85% -100%)**

Fuente: Los Autores, (ISACA, 2012)

Tabla 31

Madurez proceso APO07

PROCESO:	**APO07 GESTIONAR LOS RECURSOS HUMANOS**							
DESCRIPCIÓN:	Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.							
PROPÓSITO:	Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.							
APO07	**Evaluar si se consiguen los siguientes resultados**	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	**No Alcanzados (0-15%)**	**Parcialmente Alcanzados (15% - 50%)**	**Alcanzado en Gran Medida (50% - 85%)**	**Totalmente Alcanzado (85% - 100%)**
Nivel 0 Incompleto	El proceso no se ha implementado , o no ha logrado conseguir su propósito	En este nivel, hay pocas o ninguna evidencia del cumplimiento del propósito del proceso						
Nivel 1 Ejecutado	PA1.1 El proceso alcanza su propósito	Los siguientes resultados del proceso se están cumpliendo						
		La estructura organizacional y las relaciones de TI son flexibles y dan respuesta	No					

CONTINÚA

	ágil.		
	Los recursos humanos son gestionados eficaz y eficientemente.	Si	50%

Fuente: Los Autores, (ISACA, 2012)

Tabla 32

Calificación proceso APO10

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	NIVEL 5
APO10		PA 1.1	PA 2.1 PA 2.2	PA 3.1 PA 3.2	PA 4.1 PA 4.2	PA 5.1 PA5.2
Puntuación de los criterios		P (12%)				
Nivel de Madurez Conseguido	0					
			N (0-15%)	**P (15% - 50%)**	**L (50% - 85%)**	**F (85% - 100%)**

Fuente: Los Autores, (ISACA, 2012)

Tabla 33

Madurez proceso APO10

PROCESO:	**APO10 GESTIONAR LOS PROVEEDORES**							
DESCRIPCIÓN:	Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.							
PROPÓSITO:	Minimizar el riesgo de proveedores que no rindan y asegurar precios competitivos.							
APO10	**Evaluar si se consiguen los siguientes resultados**	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	**No Alcanzados (0-15%)**	**Parcialmente Alcanzados (15% - 50%)**	**Alcanzado en Gran Medida (50% - 85%)**	**Totalmente Alcanzado (85% - 100%)**
Nivel 0 Incompleto	El proceso no se ha implementado , o no ha logrado conseguir su propósito	En este nivel, hay pocas o ninguna evidencia del cumplimiento del propósito del proceso						
Ni 1 Ejecutado	PA1.1 El proceso alcanza su propósito	Los siguientes resultados del proceso se están cumpliendo						
		Los proveedores rinden según lo acordado.	Si	Los proveedores no siempre se rigen a lo acordado		45%		

CONTINÚA

	El riesgo de los proveedores se evalúa y trata adecuadamente.	NO
	Las relaciones con los proveedores son eficaces.	NO

Fuente: Los Autores, (ISACA, 2012)

Tabla 34

Calificación proceso BAI01

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	NIVEL 5
BAI01		PA 1.1	PA 2.1 PA 2.2	PA 3.1 PA 3.2	PA 4.1 PA 4.2	PA 5.1 PA5.2
Puntuación de los criterios						
Nivel de Madurez Conseguido	0					
			N (0-15%)	**P (15% - 50%)**	**L (50% - 85%)**	**F (85% - 100%)**

Fuente: Los Autores, (ISACA, 2012)

Tabla 35

Madurez proceso BAI01

PROCESO:	**BAI01 GESTIÓN DE PROGRAMAS Y PROYECTOS**							
DESCRIPCIÓN:	Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia Corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.							
PROPÓSITO:	Alcanzar los beneficios de negocio y reducir el riesgo de retrasos y costes inesperados y el deterioro del valor, mediante la mejora de las comunicaciones y la involucración de usuarios finales y de negocio, asegurando el valor y la calidad de los entregables del proyecto y maximizando su contribución al portafolio de servicios e inversiones.							
BAI01	**Evaluar si se consiguen los siguientes resultados**	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	**No Alcanzados (0-15%)**	**Parcialmente Alcanzados (15% - 50%)**	**Alcanzado en Gran Medida (50% - 85%)**	**Totalmente Alcanzado (85% - 100%)**
Nivel 0 Incompleto	El proceso no se ha implementado , o no ha logrado conseguir su propósito	En este nivel, hay pocas o ninguna evidencia del cumplimiento del propósito del proceso						
Nivel 1 Ejecutado	PA1.1 El proceso alcanza su propósito	Los siguientes resultados del proceso se están cumpliendo						
		Las partes interesadas relevantes están comprometidas con los programas y los proyectos.	No					

CONTINÚA

	El alcance y los resultados de los programas y proyectos son viables y están alineados con los objetivos.	No
	Los planes de programas y proyectos tienen probabilidades de lograr los resultados esperados	No
	Las actividades de los programas y proyectos se ejecutan de acuerdo a los planes.	No
	Existen suficientes recursos de los programas y proyectos para realizar las actividades de acuerdo a los planes.	No

Fuente: Los Autores, (ISACA, 2012)

Tabla 36

Calificación proceso BAI02

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	NIVEL 5
BAI02		PA 1.1	PA 2.1 PA 2.2	PA 3.1 PA 3.2	PA 4.1 PA 4.2	PA 5.1 PA5.2
Puntuación de los criterios						
Nivel de Madurez Conseguido	0					
			N (0-15%)	**P (15% - 50%)**	**L (50% - 85%)**	**F (85% - 100%)**

Fuente: Los Autores, (ISACA, 2012)

Tabla 37

Madurez proceso BAI02

PROCESO:	**BAI02 GESTIONAR LA DEFINICIÓN DE REQUISITOS**
DESCRIPCIÓN:	Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.
PROPÓSITO:	Crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan

CONTINÚA

BAI02	**Evaluar si se consiguen los siguientes resultados**	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	**No Alcanzados (0-15%)**	**Parcialmente Alcanzados (15% - 50%)**	**Alcanzado en Gran Medida (50% - 85%)**	**Totalmente Alcanzado (85% - 100%)**
Nivel 0 Incompleto	El proceso no se ha implementado , o no ha logrado conseguir su propósito	En este nivel, hay pocas o ninguna evidencia del cumplimiento del propósito del proceso						
Nivel 1 Ejecutado	PA1.1 El proceso alcanza su propósito	Los siguientes resultados del proceso se están cumpliendo						
		Los requerimientos funcionales y técnicos del negocio reflejan las necesidades y expectativas de la organización.	No					
		La solución propuesta satisface los requerimientos funcionales, técnicos y de cumplimiento del negocio.	No					
		El riesgo asociado con los requerimientos ha sido tomado en cuenta en la solución propuesta.	No					
		Los requerimientos y soluciones propuestas cumplen con los objetivos del caso de negocio (valor esperado y costes probables).	No					

Fuente: Los Autores, (ISACA, 2012)

Tabla 38

Calificación proceso DSS01

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	NIVEL 5
DSS01		PA 1.1	PA 2.1 PA 2.2	PA 3.1 PA 3.2	PA 4.1 PA 4.2	PA 5.1 PA5.2
Puntuación de los criterios		P (15%)				
Nivel de Madurez Conseguido	0					
			N (0-15%)	**P (15% - 50%)**	**L (50% - 85%)**	**F (85% - 100%)**

Fuente: Los Autores, (ISACA, 2012)

Tabla 39

Madurez proceso DSS01

PROCESO:	**DSS01 GESTIONAR OPERACIONES**							
DESCRIPCIÓN:	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.							
PROPÓSITO:	Entregar los resultados del servicio operativo de TI, según lo planificado.							
DSS01	**Evaluar si se consiguen los siguientes resultados**	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	**No Alcanzados (0-15%)**	**Parcialmente Alcanzados (15% - 50%)**	**Alcanzado en Gran Medida (50% - 85%)**	**Totalmente Alcanzado (85% - 100%)**
Nivel 0 Incompleto	El proceso no se ha implementado , o no ha logrado conseguir su propósito	En este nivel, hay pocas o ninguna evidencia del cumplimiento del propósito						
Nivel 1 Ejecutado	PA1.1 El proceso alcanza su propósito	Los siguientes resultados del proceso se están cumpliendo						
		Las actividades operativas se realizan según lo requerido y programado.	Si			30%		
		Las operaciones son monitorizadas, medidas, reportadas y remediadas.	No					

Fuente: Los Autores, (ISACA, 2012)

3.4. Resultados de evaluación de los procesos

Por medio de la evaluación realizada se ha podido obtener la madurez de los procesos en la ESPE sede Santo Domingo como se muestra en la Tabla 40:

Tabla 40

Madurez de los procesos

PROCESOS	DESCRIPCIÓN	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4	NIVEL 5
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno		P				
EDM02	Asegurar la Entrega de Beneficios		P				
EDM04	Asegurar la Optimización de Recursos						
APO01	Gestionar el Marco de Gestión de TI		P				
APO04	Gestionar la Innovación		P				
APO07	Gestionar los Recursos Humanos		P				
APO10	Gestionar los Proveedores		P				
BAI01	Gestión de Programas y Proyectos						
BAI02	Gestionar la Definición de Requisitos						
DSS01	Gestionar Operaciones		P				

Fuente: Los Autores, (ISACA, 2012)

4. INFORME

REPORTE DE AUDITORÍA INDEPENDIENTE

Universidad de las Fuerzas Armadas ESPE

ESPE Sede Santo Domingo

Nov 2014 – Abril 2015

20 de Mayo del 2015

Señores ESPE sede Santo Domingo

Evaluación y Auditoria - ESPE

Por medio del presente informe presentamos los resultados de la Evaluación Técnica a al área de tecnología de la Universidad de las Fuerzas Armadas – ESPE, Santo Domingo. Esta auditoría se llevó en el periodo Nov 2014 – Abril 2015. Para realizar el presente informe utilizamos como Marco de Referencia COBIT 5, y analizaron los procesos considerados de mayor criticidad o importancia.

El presente informe ha sido redactado bajo guía de referencia, IS Audit and Assurance Standards y IS Audit and Assurance Guidelines issued by ISACA, con las evidencias y resultados se dan recomendaciones o directrices que mejoren la parte de gobierno, gestión, y operatividad de TI. Este informe concluye el alcance de los objetivos de auditoría planteados al inicio de la Evaluación.

Auditores:

Ing. Margoth Guaraca,

Ing. Paulina Ayala

4.1. Introducción

La Universidad de las Fuerzas Armadas – ESPE, forma parte del Sistema de Educación Superior del Ecuador, es una institución que posee autonomía administrativa, personería jurídica y patrimonio propio, de derecho público, está compuesta por: la sede matriz está ubicada en la provincia de Pichincha, ciudad Sangolquí, y ESPE Santo Domingo ubicada en la provincia Santo Domingo de los Tsáchilas, ciudad Santo Domingo.

La ESPE sede Santo Domingo forma parte importante en el desarrollo de la región formando profesionales entregados y responsables en la carrera de Ingeniería Agropecuaria (IASAII) actualmente se encuentra en un proceso de Evaluación y

Acreditación y para eso se han ejecutado varios cambios a nivel institucional entre ellos, el modelo educativo, estructura organizacional y procesos de gestión institucional donde la Unidad de Tecnologías de Información y Comunicación facilita por medio del uso de las TIC el proceso de enseñanza aprendizaje a los estudiantes, además permite centralizar y administrar los procesos administrativos y académicos de forma adecuada.

La ESPE Santo Domingo está entrando a un proceso cambio, acreditación y ampliación de la oferta académica lo que significaría que se debe fortalecer el área de TI para que brinde un adecuado soporte a este proceso y esto se pude lograr primero con la evaluación a la Unidad de Tecnología que permitirá saber el alcance de los procesos.

4.2. Objetivos de Auditoría

Los objetivos de la Evaluación Técnica Informática que se detallan en este informe son los mismos que están descritos en las páginas preliminares de este documento

Objetivo General

Realizar una evaluación técnica informática a la parte tecnológica de la ESPE – Sede Santo Domingo en base a riesgos utilizando como marco de referencia COBIT5.

Objetivos específicos

- Valorar la situación actual del área tecnológica de la ESPE – Sede Santo Domingo.
- Determinar los procesos críticos en base a COBIT5, los mismos que serán evaluados.
- Ejecutar la evaluación técnica informática de la situación actual de la parte tecnológica de la ESPE – Sede Santo Domingo con respecto a lo que recomienda COBIT5 de los procesos seleccionados.

- Realizar informe en base a riesgos con las respectivas recomendaciones pertinentes en base a lo que recomienda el modelo COBIT5 para las no conformidades y hallazgos respectivos.

4.3. Metodología de Auditoría

Plan de auditoria

Para determinar los objetivos y alcance de la auditoría, se revisó el plan estratégico de la Universidad de Fuerzas Armadas ESPE, vigente para el periodo 2014-2017, el mismo que realizó un cruce con el modelo en cascada de COBIT 5, para determinar las metas de TI asociadas a los objetivos de la organización y luego se determinaron los procesos de mayor criticidad a ser evaluados el mismo que fueron respaldados en reuniones de trabajo realizados al Director de la ESPE sede Santo Domingo y el Mg. Eduardo Benavides encargado de los laboratorios de la institución. También se realizó una investigación preliminar de campo con una observación directa en donde se determinó la situación actual de la parte tecnológica de la sede.

Nuestro plan de auditoría incluye las siguientes fases:

1. Investigar y analizar información referente a COBIT 5 y riesgos informáticos.

2. Recabar y analizar la información referente a la parte tecnológica de la ESPE – Santo Domingo.

3. Determinar los procesos más críticos y relevantes en base a los objetivos estratégicos de la ESPE, que serán objeto de la evaluación.

4. Ejecutar la auditoria en base a los procesos y actividades preseleccionadas con COBIT 5, en base a los objetivos estratégicos de la institución.

5. Analizar los riesgos presentes de la parte tecnológica de la institución

6. Elaborar el informe de la evaluación técnica informática en base a los riesgos encontrados.

4.4. RESULTADOS DE AUDITORÍA

A continuación se presenta los hallazgos obtenidos de la evaluación realizada a la parte tecnológica de la Universidad de las Fuerzas Armadas ESPE sede Santo Domingo con COBIT 5, la misma que se basó en la selección de procesos de mayor criticidad.

1. **PROCESO: EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.**

   Condición:

   Se encontró que no hay un diseño de gobierno que tome en cuenta los factores del entorno interno y externo, que esté alineado a TI y a los requerimientos de las partes interesadas, además no se cuenta con un plan estratégico diseñado para el entorno local, se rigen únicamente al plan estratégico institucional de la sede Matriz.

   Se evidenció que no existe un diseño de gobierno de TI, solo existe una entidad relacionada a tecnología que en el organigrama institucional se lo presenta como área de "Laboratorios" en donde por encargo interno lo administra un docente de la institución además, no se tienen definidos roles, responsabilidades, autoridades asignados y aceptados para una gestión TI apropiados.

   EL sistema de gobierno actual de la organización no ha evaluado a TI, y al no existir un área de TI no hay gobierno de TI, en base a estos hechos se determina que la parte tecnológica no opera de forma eficiente.

Criterio

La institución debe tener un modelo estratégico de toma de decisiones para que las TI sean efectivas y estén alineadas con el entorno externo e interno de la empresa y los requerimientos de las partes interesadas.

Se debe garantizar que el sistema de gobierno para TI está incorporado al gobierno corporativo.

Se debe obtener garantías de que el sistema de gobierno para TI está operando de manera efectiva.

Causa:

No hay establecida un área de TI a nivel de la sede, tampoco cuenta con un plan estratégico, políticas y procedimientos con sus respectivos roles y responsabilidades que respalden sus operaciones y servicios en la institución y que esté alineados a la misión de la ESPE - Matriz.

Riesgo - Efecto

Al no existir un diseño de gobierno que esté alineado a TI, no se asegura que se cumpla con los requerimientos de las partes interesadas y podría estar desperdiciando recursos relacionados a TI.

En cuanto a tecnología se depende totalmente del departamento denominado UTICs, de la sede matriz quienes son los que realizan las tareas de instalación, soporte y mantenimiento, derivando en un servicio poco adecuado y que podría paralizar las actividades o servicios de la sede relacionadas con tecnología.

Recomendación:

Se debe identificar y tomar en cuenta los factores del entorno internas y externas para el diseño de gobierno que esté alineado a TI y cumplan con los requerimientos de las parte interesadas. Se debe dar la relevancia adecuada a TI con respecto al negocio. Se recomienda contratar consultoría especializada que

permita definir y guiar la implantación de un área de TI con su respectivo gobierno apropiado a las necesidades de las partes interesadas.

Definir claramente un sistema de gobierno de TI el mismo que debe estar incorporado y alineado al sistema de gobierno de la institución, el diseño de gobierno debe incluir políticas y procedimientos, roles responsabilidades que garanticen una gestión eficiente de TI.

2. PROCESO: EDM02 Asegurar la Entrega de Beneficios

Condición:

Se evidenció una falta de comprensión de los elementos clave de gobierno necesarios para la entrega fiable, segura y coste efectiva de un valor óptimo por el uso de servicios que dependen de TI.

No existen estrategias de TI local por lo cual no existe el alineamiento de TI con lo de las empresa y no se puede determinar la necesidad de integración de la partes.

Falta de control sobre incidentes que ocurren debido a la actual o tentativa de evasión de los principios y prácticas de gestión del valor establecido.

Criterio:

La empresa debe asegurar un valor óptimo de su portafolio de iniciativas TI, servicios y activos aprobados.

Se debe obtener un valor óptimo de la inversión de TI mediante prácticas de gestión del valor en la empresa.

Causa:

No existe un área de TI definido que cuente con un portafolio de iniciativas de TI, servicio y activos.

No existen prácticas de gestión del valor de la institución que permitan obtener un valor óptimo de la inversión de TI.

Riesgo - Efecto:

No se podría asegurar un valor óptimo de los servicios que ofrece TI.

No se podría determinar si se evaden los principios y práctica de gestión de valor que debería estar establecido.

Recomendación:

Comprender los requerimientos de las partes interesadas; temas estratégicos de TI, como son la dependencia de la tecnología y sus capacidades, también la importancia actual y potencial de TI para la estrategia de la empresa.

Evaluar constantemente las inversiones, servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa que aportan valor a un coste razonable.

Orientar los principios y las prácticas de gestión de valor para posibilitar la realización del valor óptimo de las inversiones TI a lo largo de todo su ciclo de vida económico

3. PROCESO: EDM04 Asegurar la Optimización de Recursos

Condición:

La asignación de recursos para TI y sus capacidades en la sede Santo Domingo se lo hace en base a proyectos propuestos y aprobados.

La asignación de recursos para TI está dada por la sede Matriz en base a presupuesto y también por gestión propia interna de la institución. Además, No existen principios normados y documentados que guíen la gestión de recursos de TI y sus capacidades.

Si bien la asignación de recursos se realiza en base a proyectos, no existe una evaluación que indique el porcentaje de proyectos que han tenido una asignación de recursos adecuado y no existen definidos indicadores o parámetros que garanticen la supervisión del uso óptimo de los recursos.

Criterio:

Las necesidades de recursos de la empresa son cubiertas con capacidades óptimas.

Los recursos se asignan para satisfacer mejor las prioridades de la empresa dentro del presupuesto y restricciones.

El uso óptimo de los recursos se logra a lo largo de su completo ciclo de vida económico.

Causa:

No hay establecido una guía la gestión de recursos de TI y sus capacidades con principios normados y documentados.

No existe un plan de recursos de TI aprobados que permita la entrega de valor y mitigación de los riesgos con los recursos asignados.

Riesgo – Efecto:

Puede haber una asignación de recursos inadecuada a proyectos sin relevancia que no aporten valor.

Existe el riesgo de que proyectos en ejecución que si aportan valor a la institución se queden sin recursos y no permitan alcanzar los objetivos planteados.

Recomendación:

Definir los principios para guiar la asignación y gestión de recursos y capacidades de manera que las TI pueda satisfacer las necesidades de la

empresa, con la habilidad y capacidad requerida de acuerdo a las prioridades acordadas y las limitaciones presupuestarias.

Revisar y aprobar el plan de recursos y las estrategias de arquitectura de la empresa para la entrega de valor, la mitigación de riesgos con los recursos asignados y supervisar la asignación y optimización de recursos de acuerdo con los objetivos y prioridades de la empresa

Definir los objetivos, medidas y métricas clave para la gestión de los recursos.

4. PROCESO : APO01 Gestionar el Marco de Gestión de TI

Condición:

No existen definidos y documentados Políticas procedimientos, las funciones, roles internos externos y las actividades de TI realizados por terceros. No se tiene establecido la implicación de las partes interesadas para la toma de decisiones críticas.

No se tiene establecido y documentado los roles y responsabilidades relativos a TI acorde a las necesidades de la empresa. Tampoco existen delimitadas claramente las responsabilidades y la rendición de cuentas en la toma y aprobación de decisiones.

Criterio:

Se ha definido y se mantiene un conjunto eficaz de política.

Todos tienen conocimiento de las políticas y de cómo deberían implementarse.

El uso óptimo de los recursos se logra a lo largo de su completo ciclo de vida económico.

Causa:

En la sede la parte tecnológica no tiene la relevancia que debería, debido a que depende directamente de la unidad UTICs de sede matriz en cuanto a recursos y gestión, se hacen visitas únicamente en caso de problemas.

Riesgo – Efecto:

Está dinámica de trabajo no garantiza que se pueda lograr los objetivos de la institución y los requisitos del gobierno corporativo.

Recomendación:

Definir el alcance, las funciones internas y externas, los roles internos y externos, y las capacidades y los derechos de decisión requeridos, incluidas actividades de TI realizadas por terceras partes

Establecer la implicación de las partes interesadas críticas para la toma de decisiones (quiénes rendirán cuentas, quiénes son responsables, quiénes deben ser consultados y quiénes informados).

Establecer, acordar y comunicar roles y responsabilidades relativos a TI para todo el personal de la empresa, de acuerdo con las necesidades y los objetivos del negocio. Delimitar claramente las responsabilidades y la rendición de cuentas, especialmente para la aprobación y toma de decisiones.

Incluir en las descripciones de roles y responsabilidades, la adhesión a las políticas y los procedimientos de gestión, al código ético y a las prácticas profesionales.

Implementar prácticas de supervisión adecuadas para garantizar que los roles y las responsabilidades se pongan en práctica de forma correcta, para evaluar si todo el personal tiene suficiente autoridad y recursos para llevar a cabo sus roles y responsabilidades y para hacer una revisión general del rendimiento. El nivel de supervisión debería estar en consonancia con la sensibilidad del puesto y el nivel de responsabilidades asignadas.

5. PROCESO : APO04 Gestionar la innovación

Condición:

No hay un plan de innovación establecido que tome en cuenta el área de TI, el apetito del riesgo, presupuesto y los objetivos que se quieren alcanzar con la innovación.

No existen políticas que permitan incentivar a la innovación utilizando tecnologías emergentes ni a supervisión sistemática que permita realizar un escaneo del entorno para identificar tecnologías emergentes que tengan el potencial de crear valor.

Criterio:

El valor de empresa es creado mediante la cualificación y puesta en escena de los avances e innovaciones tecnológicas más apropiadas, los métodos y las soluciones TI utilizadas.

Los objetivos de la empresa se cumplen por la mejora de los beneficios de la calidad y/o la reducción de costes como resultado de la identificación e implementación de soluciones innovadoras.

La innovación se permite y se promueve y forma parte de la cultura de la empresa.

Causa:

En la sede la parte tecnológica no tiene la relevancia que debería, debido a que depende directamente de la unidad UTICs de sede matriz en cuanto a recursos y gestión.

Riesgo – Efecto:

Al no contar con plan de innovación que esté apoyado en TI, se podría restar valor a la institución y no estar a nivel competitivo que la competencia a nivel local.

Recomendación:

Se debe crear un plan de innovación que acorde a las necesidades de entorno local que incluya el apetito por el riesgo, el presupuesto previsto para invertir en la innovación y los objetivos de la innovación., proveer de una infraestructura que pueda permitir innovar, tales como herramientas de colaboración para mejorar el trabajo entre diferentes ubicaciones geográficas y divisiones de la empresa.

Crear un ambiente adecuado que promueva la innovación manteniendo iniciativas de recursos humanos relevantes, tales como programas de reconocimiento a la innovación, una rotación apropiada en los puestos de trabajo y tiempo prudencial para la experimentación. Mantener un programa que permita a los empleados presentar ideas innovadoras y crear una estructura adecuada de toma de decisiones para evaluar y aplicar estas ideas. Animar a innovar a los clientes, proveedores y socios comerciales.

Implementar políticas que permitan realizar definir cuellos de botella en donde se puedan mejorar utilizando tecnologías emergentes.

6. PROCESO : APO07 Gestionar los Recursos Humanos

Condición:

No existen principios rectores para asignación de recursos y capacidades. No existen evaluaciones que permitan determinar las necesidades de talento humano en TI.

El personal de TI consiste únicamente de un docente que por encargo interno de la institución, realiza tareas de gestión de la parte tecnológica, no es suficiente para apoyar de manera apropiada los procesos de negocio e iniciativas de TI.

No existen principios de rotación de personal.

No se tiene determinado cuantos puestos de TI debe tener la institución el mismo que debe ir de acuerdo al personal total entre docente y administrativo que posee la institución.

Criterio:

La estructura organizacional y las relaciones de TI son flexibles y dan respuesta ágil.

Los recursos humanos son gestionados eficaz y eficientemente.

Causa:

Al no existir una unidad de TI definida, no se ha determinado la cantidad de personal debe ir acorde a las necesidades de la institución.

Riesgo – Efecto:

Puede ocurrir que por falta de personal con disponibilidad inmediata o por falta de personal capacitado que estén bien definidos en base a roles y responsabilidades los servicios críticos presenten incidente que afecten el alcance de los objetivos institucionales.

Recomendación:

Evaluar las necesidades de personal de TI de forma inmediata y luego 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 y objetivos empresariales.
- La empresa cuenta con recursos suficientes para apoyar de manera adecuada y apropiada los procesos de negocio y los controles e iniciativas TI.

- Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. Revisar la planificación de la sucesión.

7. PROCESO : APO10 Gestionar los proveedores

Condición:

La Universidad de las Fuerzas Armadas – ESPE. Tiene el "REGLAMENTO INTERNO DE ADQUISICIONES, CONTRATACIÓN DE SERVICIOS Y EJECUCIÓN DE OBRAS" que rige de forma general para toda la institución y las sedes donde se detallan las normas y procedimientos en la programación y ejecución de adquisición de bienes, ejecución de obra, prestación de servicios no regulados por la Ley de Consultoría, ni por el Art. 4 de la Codificación de la Ley de Contratación Pública que rige para las instituciones públicas del país, pero, no se tienen establecidos criterios de evaluación de contratos y proveedores que permitan una revisión general del rendimiento de los proveedores de manera consistente. Tampoco existe porcentaje que indique el nivel de cumplimiento de los requisitos acordados por parte de los proveedores. Además, no existen reportes que indiquen las infracciones de servicio causados por proveedores.

No existe un análisis de riesgo de los proveedores que conduzcan a incidentes en el servicio prestado. Además, no se realizan reuniones periódicas para gestionar los riesgos inherentes al servicio. Tampoco se tiene determinado el porcentaje de incidentes relacionados con el riesgo que hayan sido resueltos adecuadamente (tiempo y coste).

Criterio:

Los proveedores rinden según lo acordado.

El riesgo de los proveedores se evalúa y trata adecuadamente.

Las relaciones con los proveedores son eficaces.

Causa:

Si bien existe en el "REGLAMENTO INTERNO DE ADQUISICIONES, CONTRATACIÓN DE SERVICIOS Y EJECUCIÓN DE OBRAS" está definida una evaluación, únicamente se hace al plan anual de contrataciones que presenta todas la unidades de la ESPE, y un reporte de ingresos y egresos relacionados con la ejecución del plan de adquisiciones.

Riesgo – Efecto:

Al no tener definido y documentado los parámetros base que deben ser evaluados los proveedores no se puede garantizar, ni supervisar la calidad del servicio que ofrecen los proveedores, tampoco se pueden tener reportes de incidentes de incumplimiento que pueden afectar los servicios críticos que ofrece la institución.

Recomendación:

Establecer y mantener criterios relativos al tipo, relevancia y criticidad de los contratos con proveedores, focalizándose en aquellos de mayor importancia. Establecer y mantener un criterio de evaluación de contratos y proveedores que permita una revisión general del rendimiento de los proveedores de manera consistente. Se debe implementar un control que permita determinar el nivel de cumplimiento de los requisitos por parte de los proveedores. Registrar las infracciones de servicio que sean causados por proveedores.

Identificar, supervisar y, cuando sea apropiado, gestionar los riesgos relacionados con la capacidad del proveedor de entregar el servicio de forma eficiente, eficaz, segura, fiable y continua. A la hora de definir el contrato, incluir una descripción clara de todos los requisitos de servicio, incluyendo depósitos de garantía, proveedores alternativos o acuerdos en suspenso para mitigar el riesgo de un posible fallo del proveedor; los aspectos de seguridad, la propiedad intelectual y los requisitos legales y regulatorios.

Supervisar y revisar la entrega de servicios para asegurar que el proveedor está proporcionando una calidad del servicio adecuada, cumpliendo los requisitos y las condiciones de los contratos. Definir y documentar los criterios para supervisar el rendimiento de los proveedores alineado con los acuerdos de nivel de servicio y asegurando que el proveedor informa según estos criterios de forma regular y transparente.

8. PROCESO : BAI01 Gestión de Programas y Proyectos

Condición:

No se tiene definido planes de programas y proyectos a nivel local por tanto no se puede determinar las probabilidades de éxito.

Las parte interesadas supervisan de forma limitada si la ejecución de los programas y proyectos está acorde a lo establecido en los planes.

Los recursos asignados a los programas y proyectos vienen de dos fuentes que son: la ESPE Matriz y la sede Santo Domingo, no está claramente definido la asignación de recursos para los diferentes programas y proyectos.

Al no manejar un plan de programas y proyectos los beneficios esperados se los determina de manera empírica y no se puede determinar el porcentaje real de beneficios obtenidos y aceptados.

Criterio:

Las partes interesadas relevantes están comprometidas con los programas y los proyectos

El alcance y los resultados de los programas y proyectos son viables y están alineados con los objetivos.

No se tiene definido el alcance, los resultados de los programas y proyectos relacionados en tecnología por lo tanto el alineamiento con los objetivos organizacionales es limitado.

Los planes de programas y proyectos tienen probabilidades de lograr los resultados esperados.

Las actividades de los programas y proyectos se ejecutan de acuerdo a los planes.

Existen suficientes recursos de los programas y proyectos para realizar las actividades de acuerdo a los planes.

Los beneficios esperados de los programas y proyectos son obtenidos y aceptados.

Causa:

Al no existir un área de TI, la gestión de proyectos relacionados a TI lo realizan de forma informal, el desarrollo de programas y proyectos relacionados con tecnología no están acordes a las necesidades de la institución local, hasta la fecha la parte tecnológica depende directamente de las UTICs de la ESPE.

Riesgo – Efecto:

Podría ocurrir que los programas y proyectos desarrollados no están enfocados y alineados con la estrategia institucional, y haya un desperdicio de recursos.

Recomendación:

Las partes interesadas deben comprender la importancia de establecer un área local de TI, que sea el encargado de la gestión de programas y proyectos relacionados a TI. Definir y establecer un enfoque estándar de gestión de programas y proyectos que estén alineados a las necesidades de la institución y las buenas prácticas relacionadas. Establecer un portafolio de proyectos locales que sea gestionado de forma adecuada.

El área de TI, deberá presentar el alcance, los resultados y la viabilidad de los programas y proyectos, además deben estar alineados con los objetivos estratégicos de la institución.

Definir y documentar el plan de programas cubriendo todos los proyectos, incluyendo lo que sea necesario para lograr cambios en la empresa; su imagen, productos y servicios, procesos de negocio, habilidades y cantidad de personal, requerimientos tecnológicos, relaciones con las partes interesadas, clientes, proveedores, entre otros, así como las reestructuraciones organizacionales necesarias para lograr los resultados que la empresa espera del programa.

Especificar claramente los casos para la asignación de recursos a los diferentes programas y proyectos a ejecutar los mismos que deben estar sujetos al presupuesto.

Definir y mantener el plan de programa para asegurar que esté actualizado y refleje su alineamiento con los objetivos estratégicos actuales, el nivel de avance y los cambios materiales en los resultados, beneficios, costes y riesgos. La empresa tiene que difundir los objetivos y priorizar los trabajos para asegurar que el programa diseñado satisfará los requerimientos de la empresa. Revisar el avance de los proyectos individuales, ajustándolos si fuera necesario para satisfacer las entregas planificadas.

9. PROCESO : BAI02 Gestionar la Definición de Requisitos

Condición:

No existen definidos y documentados los requerimientos funcionales y técnicos del negocio que reflejen las necesidades y expectativas de la institución. No existen políticas y procedimientos de integridad, seguridad de datos.

No se puede determinar el nivel de cumplimiento de los requerimientos funcionales, técnicos y de cumplimiento del negocio.

En los diferentes programas y proyectos no se realiza la gestión de riesgos que puedan tener un impacto negativo en la solución propuesta.

Al no tener definido un plan de programas y proyectos se corre el riesgo que las propuestas no cumplan con los objetivos del caso de negocio.

Criterio:

Los requerimientos funcionales y técnicos del negocio reflejan las necesidades y expectativas de la organización.

La solución propuesta satisface los requerimientos funcionales, técnicos y de cumplimiento del negocio.

El riesgo asociado con los requerimientos ha sido tomado en cuenta en la solución propuesta.

Los requerimientos y soluciones propuestas cumplen con los objetivos del caso de negocio (valor esperado y costes probables).

Causa:

Debido a que la institución depende de la Sede matriz, de forma local no han visto la necesidad de realizar la definición de requerimientos funcionales y técnicos del negocio acorde a las partes interesadas.

Riesgo – Efecto:

Esto podría provocar que no estén acordes a la necesidad del entorno local y no estén alineados entre las necesidades y expectativas de la institución. Además podría comprometer la seguridad de los datos

Recomendación:

Definir e implementar la definición de requerimientos y el procedimiento de mantenimiento acorde al tamaño, complejidad, objetivos y riesgos de la iniciativa que la empresa está considerando acometer. Definir y comunicar las políticas y procedimientos de integridad y seguridad de datos.

Especificar y priorizar la información, los requerimientos técnicos y funcionales basados en los requerimientos de las partes interesadas. Incluir requerimientos de control de la información en los procesos de negocio, procesos automatizados y entornos de TI para hacer frente a los riesgos de la

información y cumplimiento con regulaciones, leyes y contratos comerciales. Incluir una evaluación de su viabilidad técnica y económica.

Involucrar a las partes interesadas para crear una lista potencial de requerimientos técnicos, funcionales, de calidad y riesgos relativos al procesamiento de la información (debido por ejemplo a falta de involucración de los usuarios, expectativas irreales, desarrolladores añadiendo funcionalidad innecesaria). Analizar y priorizar los riesgos de los requerimientos conforme probabilidad e impacto.

Al plantear los programas y proyectos se lo debe proponer como casos de negocio definir parámetros para que se cumplan los objetivos propuestos.

10. PROCESO : DSS01 Gestionar Operaciones

Condición:

No se evidenció un plan operativo para TI, en el que se detalle los procedimientos operativos y actividades relacionadas que sirva de apoyo a los servicios prestados por la parte tecnológica.

El cableado estructurado que posee la institución es mixto, hay partes que está bajo tierra o protegido (oficinas), y al cambiar de edificio va por el aire sin ninguna protección.

Criterio:

Las actividades operativas se realizan según lo requerido y programado.

Las operaciones son monitorizadas, medidas, reportadas y remediadas.

Causa:

Se debe a que no existe un plan operativo definido para la parte tecnológica que garantice la continuidad del servicio.

Riesgo – Efecto:

Al no tener un plan operativo definido se corre el riesgo de no prever desastres naturales y causados por el ser humano que puedan afectar las instalaciones de TI.

Recomendación:

Examinar los requerimientos de las instalaciones de TI respecto de la protección frente a la fluctuación y cortes de la energía eléctrica, en relación con otros requerimientos de la planificación de la continuidad del negocio. Disponer de equipamiento adecuado de alimentación ininterrumpida (p. ej. baterías, generadores) para dar soporte a la planificación de continuidad del negocio.

Establecer un plan operativo informático que incluya: misión, visión, situación actual, recursos humanos, hardware, software, problemática actual, que permita la continuidad del negocio.

CONCLUSIONES

Durante la evaluación técnica informática desarrollada en la institución se obtuvo una tabla con los procesos críticos de la institución, resultado del análisis de las diferentes matrices que nos proporciona COBIT 5 (Apéndices B, C) donde se relacionan las Metas Corporativas con las estrategias de la ESPE, las metas Corporativas con las metas de TI y por ultimo las metas de TI con los procesos, los procesos críticos arrojados por esta evaluación fueron los objetos de estudio.

En el Plan de Auditoría se definió la metodología, los objetivos, el alcance de la evaluación y los instrumentos a utilizar, en el Plan de Auditoría se seleccionaron los procesos de mayor criticidad o relevancia tomando en cuenta la opinión del Tcrn. Agr. Efrén Cisneros Director de la ESPE sede Santo Domingo y Mg. Eduardo Benavides Docente encargado de los laboratorios, los procesos seleccionados fueron, EDM01, EDMO02, EDM04, APO01, APO04, APO07, APO10, BAI01, BAI02, DSS1.

En la ejecución de auditoría se encontró principalmente que la sede Santo Domingo no dispone de un área de TI definida y establecida formalmente con directrices políticas, procedimientos, roles y responsabilidades que sirvan para dar un soporte adecuado al alcance de los objetivos estratégicos de la institución y los requerimientos de mantenimiento y soporte local.

Finalmente se elaboró el informe bajo la Guía de Referencia, IS Audit and Assurance Standards y IS Audit and Assurance Guidelines issued de ISACA, con los hallazgos, criterios de evaluación, causa, efecto – riesgo, y las recomendaciones pertinentes para cada proceso evaluado. Como se indicó anteriormente al no disponer de un área de TI, el principal riesgo es que se vea afectada la continuidad de los servicios que ofrecen la universidad y dependen directamente de TI.

RECOMENDACIONES

Se recomienda realizar e implementar todas la recomendaciones dadas en el informe de auditoría y principalmente la de implantar un área de TI local que permita dar soporte y mantenimiento a los servicios y equipos de la institución y principalmente permita el alineamiento con las metas de la institución.

Al realizar la implementación se recomienda utilizar COBIT 5 como marco de referencia que permitan lograr una alineación adecuada entre las metas corporativas y las metas de TI, tomando en cuenta las particularidades de la institución debido que COBIT 5 no es una camisa de fuerza sino más bien una guía adaptable a los requerimientos y necesidades de cada institución.

Se debería tomar medidas de control para los riesgos presentados en el informe final, para evitar inconvenientes en el funcionamiento de la Sede, especialmente mientras dure la implantación del área de TI.

Se recomienda tomar como base el presente estudio para futuras evaluaciones que se realicen a la sede Santo Domingo y profundizar en los procesos de Adquisición, Construcción e Implementación y Entrega, Servicio y Soporte considerados en los procesos catalizadores de COBIT 5.

Bibliografía

Burlaung, N. (2014). *ESPE*. Obtenido de http://www.espe.edu.ec/

Hernández Hernández, E. (2002). *Auditoría en Informática.* México: CECSA.

ISACA. (2012). *COBIT 5.* Obtenido de www.isaca.org

Piattini Velthius, M., del Peso Navarro, E., & del Peso Ruiz, M. (2008). *Auditoría de Tecnologías y Sistemas Información.* Madrid, España: Ra-Ma.

Piattini, M., & Del Peso, E. (2001). *Auditría Informática Un enfoque práctico.* Bogotá: Alfaomega - RaMa.

Quishpe Goyes, B. E., & Vargas Cisneros, M. S. (2013). *Modelo de Auditoría Informática Basada en Riesgos en Ámbitos Financieros.* Quito: Escuela Politécnica Nacional.

ANEXO 1 Plan Estratégico Institucional ESPE 2014-2017

ANEXO 2 Tablas Selección de Procesos

ANEXO 3 Acta Selección de Procesos Tcrn. Efrén Cisneros

ANEXO 4 Acta Selección de Procesos Eduardo Benavides

ANEXO 5 Plan de Auditoría

ANEXO 6 Entrevista Preliminar

ANEXO 7 Lista de Documentos a Solicitar

ANEXO 8 Respuestas cuestionario Eduardo Benavides RRHH

ANEXO 9 Respuestas cuestionario Eduardo Benavides RRHH

ANEXO 10 Respuestas cuestionario RRHH

ANEXO 11 Ficha de Observación

ANEXO 12 Respuestas cuestionario Final