ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA

CENTRO DE POSGRADO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

VII PROMOCIÓN

TEMA: "EVALUACIÓN TÉCNICA INFORMÁTICA DE LOS PROCESOS DE GOBIERNO DE TI (EVALUAR, ORIENTAR Y SUPERVISAR) AL SISTEMA DE INFORMACIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS "ESPE" SEDE PRINCIPAL."

AUTORES: GUANOTUÑA LASCANO, EMILLY JEANETTE
CHÁVEZ ÑAUÑAY, CARLOS PATRICIO

DIRECTOR: ING. RON, MARIO MSc.

SANGOLQUÍ
2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLÓGICA
CENTRO DE POSGRADO
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

CERTIFICACIÓN

Certifico que el trabajo de titulación: "**EVALUACIÓN TÉCNICA INFORMÁTICA DE LOS PROCESOS DE GOBIERNO DE TI (EVALUAR, ORIENTAR Y SUPERVISAR) AL SISTEMA DE INFORMACIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS "ESPE" SEDE PRINCIPAL**", realizado por los señores **EMILLY JEANETTE GUANOTUÑA LASCANO Y CARLOS PATRICIO CHÁVEZ ÑAUÑAY,** ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo que cumple con los requisitos teóricos, científicos, técnicos metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a los señores **EMILLY JEANETTE GUANOTUÑA LASCANO Y CARLOS PATRICIO CHÁVEZ ÑAUÑAY** para que lo sustenten públicamente.

Sangolquí, 18 de enero del 2016

Ing. Mario Ron MSc.
DIRECTOR DE TESIS

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLÓGICA
CENTRO DE POSGRADO
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

AUTORÍA DE RESPONSABILIDAD

Nosotros, **EMILLY GUANOTUÑA LASCANO**, con cédula de identidad N° 1715245815 y **CARLOS PATRICIO CHÁVEZ**, con cédula de identidad N° 0603226895, declaramos que este trabajo de titulación **"EVALUACIÓN TÉCNICA INFORMÁTICA DE LOS PROCESOS DE GOBIERNO DE TI (EVALUAR, ORIENTAR Y SUPERVISAR) AL SISTEMA DE INFORMACIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS "ESPE" SEDE PRINCIPAL"**, ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaramos que este trabajo es de nuestra autoría, en virtud de ello nos declaramos responsables del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 18 de enero del 2016

Emilly Guanotuña Lascano
CC. 1715245815

Carlos Patricio Chávez N.
CC. 0603226895

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLÓGICA
CENTRO DE POSGRADO
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

AUTORIZACIÓN

Nosotros, **EMILLY GUANOTUÑA LASCANO** y **CARLOS PATRICIO CHÁVEZ**, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación **"EVALUACIÓN TÉCNICA INFORMÁTICA DE LOS PROCESOS DE GOBIERNO DE TI (EVALUAR, ORIENTAR Y SUPERVISAR) AL SISTEMA DE INFORMACIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS "ESPE" SEDE PRINCIPAL"**, cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

Sangolquí, 18 de enero del 2016

Emilly Guanotuña Lascano
CC. 1715245815

Carlos Patricio Chávez N.
CC. 0603226895

DEDICATORIA

A Dios: Por haberme dado la vida, sabiduría y su infinita misericordia.

A mi esposa: Por su amor, comprensión y apoyo; brindados en los momentos más difíciles de mi vida.

Carlos

Dedico el presente trabajo a mis padres y hermanos, quienes han sabido apoyarme y comprender mis ausencias durante largos meses.

Emilly

AGRADECIMIENTOS

Agradecemos a Dios por darnos la vida la vida, la perseverancia y el optimismo para seguir adelante en todas las instancias de nuestras vidas, por darnos la dicha de tener cada uno de nosotros una familia maravillosa y amigos valiosos.

Un agradecimiento muy especial, al Ing. Mario Ron, Director de Tesis, por su incondicional apoyo y aporte profesional, quien con sus recomendaciones ha hecho posible la culminación de la presente tesis de grado.

Carlos y Emilly

ÍNDICE DE CONTENIDO

ÍNDICE DE CUADROS

ÍNDICE DE FIGURAS

RESUMEN

La Evaluación Técnica Informática de los Procesos de Gobierno de TI al Sistema de Información de la Universidad de las Fuerzas Armadas ESPE Matriz, utiliza el marco de referencia COBIT 5 e identifica los procesos más críticos de la Institución a través de una matriz de riesgo elaborada de acuerdo a los criterios establecidos en este marco de referencia. Se elabora un programa detallado de Auditoría, mediante una matriz de investigación de campo, en la que se detalla el objeto del análisis, los procesos, prácticas de gestión y actividades que se evalúan, así como las técnicas e instrumentos de investigación que se utilizan para la recopilación de la información pertinente, la que una vez recogida, es analizada en referencia a las buenas prácticas establecidas en el marco de referencia antes enunciado. Establecida la brecha, reconocidas causas y potenciales riesgos, se elabora el informe detallado y el ejecutivo en base del documento para reportes de Auditoría de ISACA (IS Auditing Report). Se establece en cada observación la condición, el criterio, la causa, el efecto (riesgo) y la recomendación correspondiente; en el caso de que alguno de los participantes en el proceso requiere señalar aspectos importantes y relevantes a la observación realizada se añade su punto de vista.

PALABRAS CLAVES:

- **PROCESOS DE GOBIERNO TI**
- **MARCO DE REFERENCIA**
- **EVALUACIÓN TÉCNICA**
- **ISACA**
- **COBIT 5**

ABSTRACT

Computer Technical Evaluation Process IT Governance Information System at the University of the Armed Forces ESPE Matrix, use the COBIT 5 framework and identifies the most critical processes of the institution through a risk matrix prepared in According to the criteria set out in this framework. A detailed program of Audit It is made by an array of field research, in which the object of analysis, processes, management practices and activities are evaluated, as well as techniques and research instruments used for detailed gathering relevant information, which once collected, it is analyzed in reference to good practices established in the framework enunciated above. Established gap, recognized causes and potential risks, the detailed report and the executive on the basis of the document to ISACA Audit reports (IS Auditing Report) is made. The condition, criteria, cause, effect (risk) and corresponding recommendation is set at each observation; in the event that any of the participants in the process requires important and relevant to note the observation made respects his view is added.

KEYWORDS:

- **IT GOVERNANCE PROCESS**
- **FRAMEWORK**
- **TECHNICAL EVALUATION**
- **ISACA**
- **COBIT 5**

CAPÍTULO I
INTRODUCCIÓN

1.1 Planteamiento del problema

Actualmente la Universidad de las Fuerzas Armadas ESPE sede principal, se encuentra en un proceso de cambio institucional, especialmente en el área de Gobierno de TI, con una nueva estructura organizacional, cambio permanente de autoridades y falta de información relacionada al desempeño de TI en función de estándares y buenas prácticas reconocidas a nivel nacional e internacional.

1.2 Formulación del problema.

- ¿Es suficiente y adecuada la información que tiene el nivel estratégico de la ESPE, en referencia al apoyo de TI a la Misión y Objetivos Institucionales?
- ¿Cuál es la condición actual de TI en la ESPE, considerando marcos de referencia, estándares y buenas prácticas actuales?
- ¿Cuál estándar podría ser aplicado de mejor manera para la administración de TI en la ESPE?

1.3 Justificación del problema

La ESPE es una Institución de Educación Superior en constante evolución, que ha conseguido inicialmente su calificación A, por parte del CEAACES, pero es necesario evaluar y mejorar los procesos de Gobierno de TI que en ella se realizan, con la finalidad de brindar servicios de calidad y mantener su acreditación.

El Gobierno de TI provee las estructuras que vinculan los procesos de TI, sus recursos y la información, con las estrategias y los objetivos de negocio de la Institución; además, integra e institucionaliza las mejores prácticas de planificación y organización, adquisición e implementación, entrega de servicios y soporte y monitoriza el rendimiento de TI, para asegurar que la información de la Institución y las tecnologías relacionadas soporten los

objetivos del negocio; esto conduce a la Institución a tomar total ventaja de su información, maximizar sus beneficios, capitalizar sus oportunidades y mejorar su competitividad.

Por lo expuesto es importante y necesario conocer desde un punto de vista imparcial, el estado actual de los procesos de Gobierno de TI, compararlo con las mejores prácticas que nos brindan Marcos de referencia como COBIT, ISO y otros, para establecer la brecha, que será minimizada de acuerdo a recomendaciones emitidas por un equipo de trabajo preparado técnicamente para el efecto, como son los estudiantes de la Maestría en Evaluación y Auditoría de Sistemas Tecnológicos de la ESPE.

1.4 Objetivo general

Evaluar los Procesos de Gobierno de TI de la Universidad de las Fuerzas Armadas ESPE Matriz, aplicando como marcos de referencia COBIT 5 e ITIL v.3, con el fin de crear valor para la Institución.

1.5 Objetivos específicos

- Elaborar la Planificación detallada del proyecto.
- Elaborar el Plan de Investigación de Campo en base de la Matriz de Riesgos.
- Elaborar y aplicar los Instrumentos de Investigación de campo.
- Realizar el análisis de la información.
- Redactar y presentar los informes del análisis de la Evaluación.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes

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

La Universidad de las Fuerzas Armadas ESPE, se encuentra en un proceso de cambio institucional, en el que se pretende crear una nueva estructura organizacional y las políticas y regulaciones necesarias para su funcionamiento.

La Unidad de Desarrollo Institucional, ha elaborado un proyecto para obtener información adecuada y pertinente acerca del desempeño de la Unidad de Tecnología de la Información de la ESPE y de su Sistema de Información Institucional.

2.2 ITIL

ITIL (IT infrastructure library) es un marco de referencia de mejores prácticas que ayuda a gestionar operaciones y servicios TI, se inicia a mediados de los 80, auspiciado por la Oficina de Comercio del Gobierno del Reino Unido (“Govermment of Comerce”). Durante su vida ha sufrido numerosas modificaciones y ampliaciones, pero tiene su origen en la administración de servicios informáticos.

El modelo de ITIL está basado en la provisión de servicios de manera efectiva, eficiente y controlada, pero no deja de lado la necesidad de la creación de políticas, procedimientos o controles que faciliten, normalicen y optimicen la Gestión de los Servicios.

2.2.1 Estructura de ITIL v3

Actualmente ITIL se encuentra agrupado en 5 publicaciones, cada una de ellas describe un conjunto de procesos de Gestión de Servicios IT (ver figura 1).

- **Estrategia del Servicio (Service Strategy)**
  - Garantiza que cada fase del ciclo de vida del servicio permanece orientada al negocio.
  - Afecta a lo que ocurre en el resto de las fases.
  - Se relaciona con todos los elementos asociados que le siguen dentro de ese proceso.

- **Diseño del Servicio (Service Desing)**
  - Implica el desarrollo de las especificaciones para mejorar los servicios o introducir otros nuevos.

- **Transición del Servicio (Service Transition)**
  - Somete los servicios nuevos o mejorados a controles de calidad y garantiza su adecuada puesta en producción.
  - Incluye pruebas, Gestión del cambio y Gestión del envío al entorno de producción.

- **Operación del Servicio (Service Operation)**
  - Se centra en ejecutar y controlar las actividades de los procesos para conseguir la Gestión del servicio deseable y estable en las operaciones diarias.

- **Mejora Continua del Servicio (Continua Service)**
  - Mantiene la tradición de ITIL de introducir continuas mejoras.

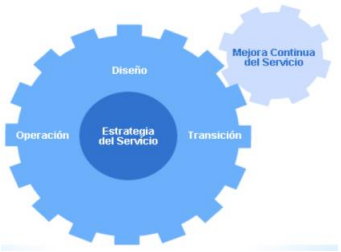

Figura 1 Estructura de ITIL v3

Fuente: (Osiatis, 2012)

2.2.2 Gestión de Servicios IT

En muchas organizaciones los roles y responsabilidades no se encuentran claramente definidos; muchos empleados tienen a su cargo responsabilidades que no competen a su función, deben tratar con incidencias, problemas, cambios y muchas veces no conocen cómo gestionarlos de mejor manera.

Actualmente los clientes exigen al personal de IT más allá de un producto final, los clientes están demandando servicio constante y estable, que el personal de IT tenga disponibilidad de atención de 24x7, que el servicio que entreguen sea de calidad, que no sólo se quede el área de IT en la ejecución de sus objetivos, sino que cubra también los objetivos de la empresa, que conozcan sus necesidades y que éstas sean convertidas en soluciones.

Este es el enfoque de Gestión de Servicio para ITIL, es una nueva manera de pensar, deseo de entregar valor añadido y valor real al cliente. Esto no se consigue en corto tiempo, es necesario proyectarse a un largo plazo para construir las mejoras en los procesos.

La Gestión de Servicio está orientada a entregar servicios de IT a los clientes permitiéndoles alcanzar los objetivos de sus Líneas de Negocio (LOB) englobados en los acuerdos de nivel de servicio (SLAs) y acuerdos de nivel operacional (OLAs).

La Gestión de Servicio implementa procesos con la orientación de ITIL como guía. ITIL proporciona un conjunto comprensivo, consistente y coherente de prácticas óptimas para los procesos de Gestión de Servicio.

2.3 COBIT

2.3.1 Historia de COBIT

COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas), fue lanzado por primera vez en septiembre de 1996, su segunda edición en abril de 1998, la tercera en marzo del 2000, la cuarta versión (COBIT 4.1) en el primer semestre del año 2007 y la última versión (COBIT 5.0) en el año 2012 (ver figura 2).

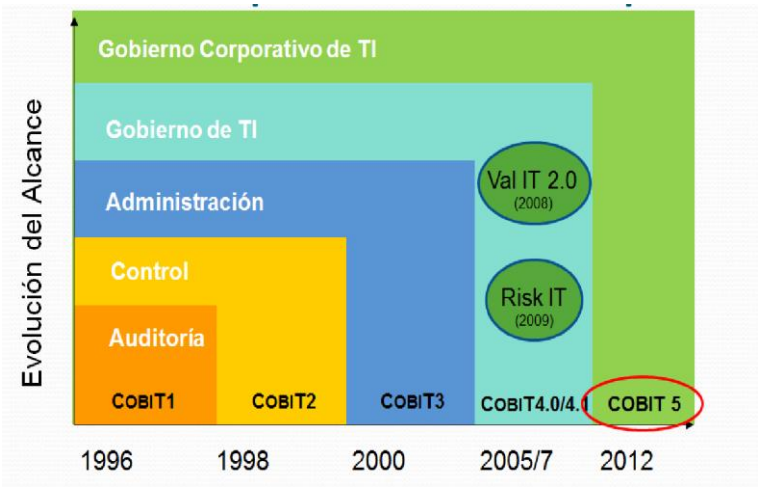

Figura 2 Evolución de COBIT

Fuente: (ISACA, 2012)

Este marco provee buenas prácticas y presenta actividades para el Gobierno de TI en una estructura manejable y lógica. Las buenas prácticas de COBIT reúne el consenso de expertos, quienes ayudan a optimizar la inversión en TI y proporcionan un mecanismo de medición que permiten juzgar cuando las actividades van por el camino equivocado.

COBIT Integra y concilia normas y reglamentaciones existentes como: ISO (9000-3), Códigos de Conducta del Consejo Europeo, COSO[3], IFAC[4], IIA[5], AICPA[6], ISACA y Otras.

2.3.2 Beneficios de COBIT 5

- Proporciona un marco de referencia amplio, que ayuda a las empresas a alcanzar sus metas y ofrecer valor a través de una gobernabilidad y Gestión eficaz de las TI en la empresa.
- Define el punto de partida de la gobernabilidad y las actividades de Gestión con las necesidades de las partes interesadas relacionadas con las TI de la empresa.
- Crea una visión más holística, integrada y completa de la gobernabilidad y Gestión empresarial de TI, esta ofrece una visión extremo a extremo en todos los aspectos relacionados a TI.
- Crea un lenguaje común entre TI y el negocio para la gobernabilidad y Gestión empresarial de las TI.
- Es consistente con los estándares de gobernabilidad corporativos generalmente aceptados y así ayuda a cumplir con los requerimientos regulatorios.

2.3.3 Procesos de Gobierno y Gestión de COBIT 5

Una de los principios de COBIT es la distinción entre Gobierno y Gestión. En esta línea y en base a este principio, se espera que todas las empresas implementen procesos que proporcionen un entorno de IT exhaustivo.

Al considerar los procesos para Gobierno y Gestión en el contexto de la empresa, se debe diferenciar cada uno de ellos de acuerdo a los objetivos que se detallan a continuación:

- **Procesos de Gobierno. -** Los procesos de Gobierno tienen relación con los objetivos de las partes interesadas: entrega de valor, optimización del riesgo y de recursos e incluye prácticas y actividades orientadas a evaluar opciones estratégicas,

proporcionando a la dirección facilidad en la toma de decisiones (ISACA, 2012).

- **Procesos de Gestión. -**En línea con la definición de Gestión, las prácticas y actividades de los procesos de gestión abarcan las áreas de responsabilidad de Planificar, Construir, Ejecutar y Supervisar (Plan, Build, Run and Monitor-PBRM) de lasTI de la empresa y tienen que proporcionar cobertura de TI extremo a extremo (ISACA, 2012).

Aunque la salida de ambos tipos de procesos es diferente y está destinada a distinta audiencia, en el contexto todos los procesos requieren actividades de: Planificación, Construcción o Implementación, Ejecución y Supervisión.

2.3.3.1 Modelo de Referencia COBIT

COBIT 5, no es preceptivo, pero por lo mencionado anteriormente está clara la necesidad de que las empresas implementen procesos de Gobierno y de Gestión, de forma que las áreas claves estén totalmente cubiertas (ver figura 3).

En teoría, una empresa puede organizar sus procesos como considere conveniente, siempre y cuando los objetivos básicos de Gobierno y Gestión estén alineados con los objetivos de la Empresa.

Las pequeñas empresas tendrán menos procesos, empresas grandes y complejas tendrán más procesos.

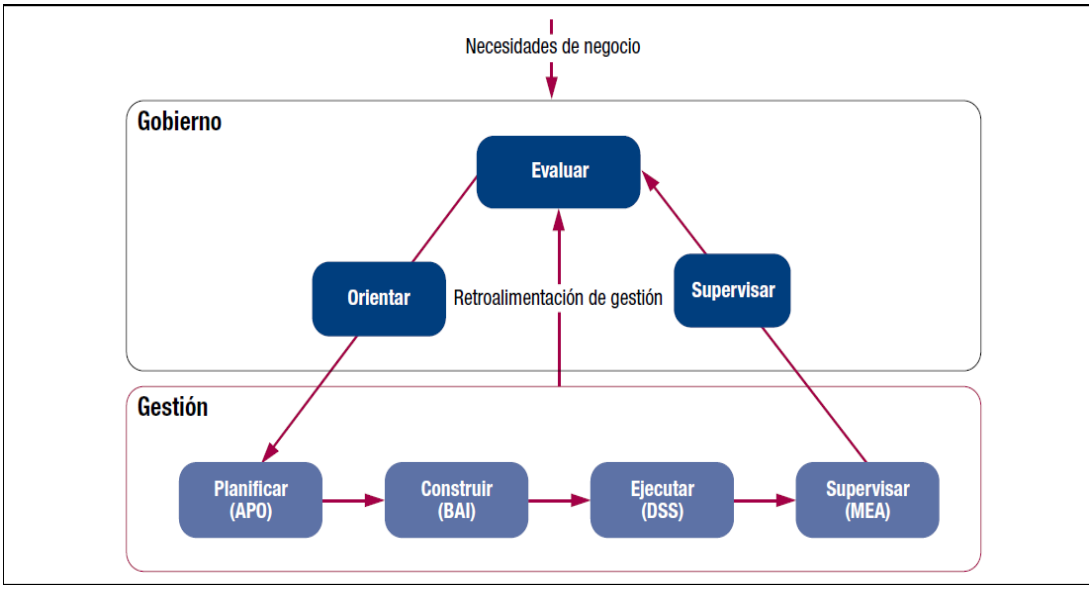

Figura 3 Áreas Clave de Gobierno y Gestión de COBIT 5
Fuente: (ISACA, Cobit 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, 2012)

2.3.3.2 Principios y Catalizadores de COBIT 5

Los principios y habilitadores o Catalizadores de COBIT 5 son genéricos y útiles para las Organizaciones de cualquier tipo, bien sean públicas, privadas, comerciales, sin fines de lucro.

2.3.3.2.1 Principios de COBIT 5

Los principios de COBIT 5 son reglas que deben seguir para gobernar o gestionar efectivamente su información y su tecnología (ISACA, Principios de COBIT 5 para el gobierno efectivo de TI, 2012).

COBIT 5 tiene cinco principios que permite construir un marco de referencia enfocado en la gobernanza y la administración eficaz, los cuales se describen en la siguiente figura (ver figura 4).

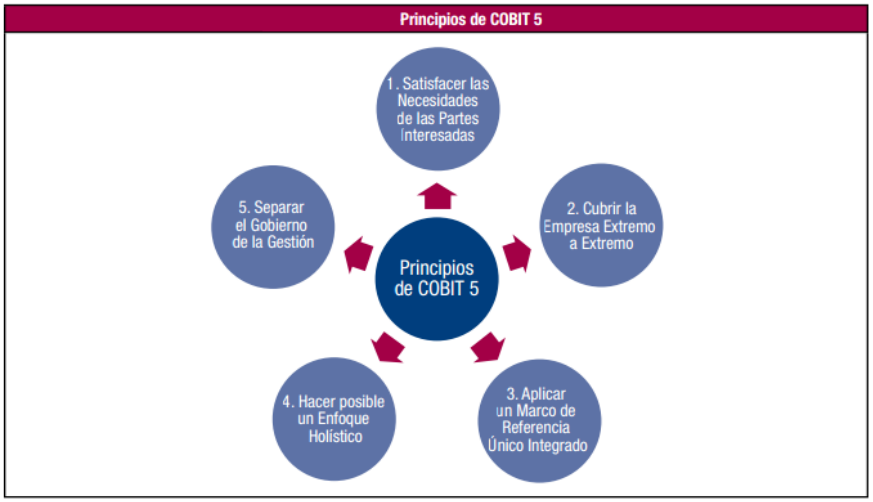

Figura 4 Principios de COBIT 5
Fuente: (ISACA, Cobit 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, 2012)

- Principio 1: Satisfacer las Necesidades de las Partes Interesadas
- Principio 2: Abarcar la Empresa de Extremo a Extremo
- Principio 3: Aplicar un Marco de Referencia Integrado Único
- Principio 4: Habilitar un Enfoque Holístico
- Principio 5: Separar Gobierno de Gestión

2.3.3.2.2 Catalizadores de COBIT 5

"Los catalizadores son factores que, individual y colectivamente, influyen sobre si algo funcionará" (ISACA, COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, 2012)

Los catalizadores COBIT 5 son:

- Factores que influyen individual y colectivamente de si algo funcionará
- Impulsados por la cascada de objetivos
- Descritos por el marco de referencia de COBIT 5 en siete categorías (ver figura 5).

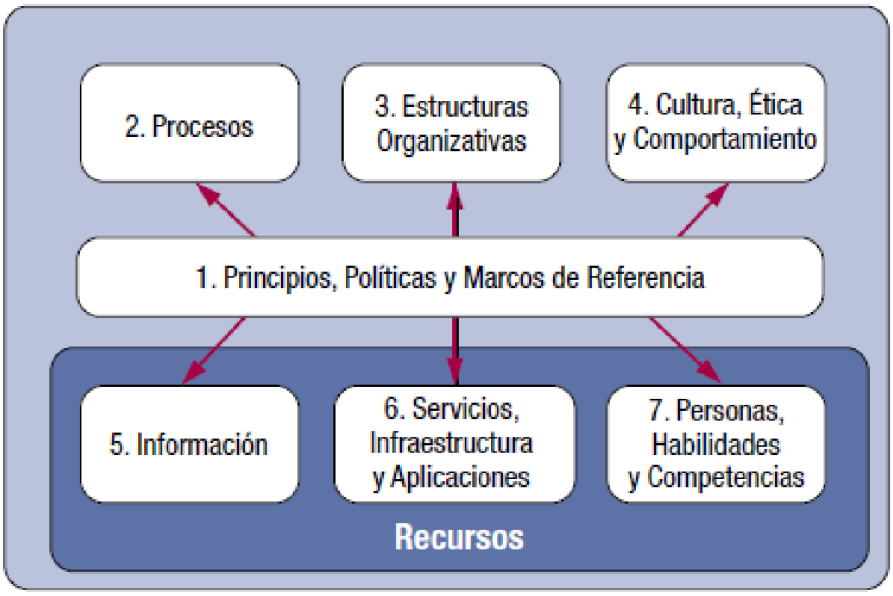

Figura 5. Facilitadores de COBIT 5
Fuente:(ISACA, COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, 2012)

1. Principios, Políticas y Marcos de Trabajo
2. Procesos
3. Estructura Organizacional
4. Cultura, Ética y Comportamiento
5. Información
6. Servicios, Infraestructura y Aplicaciones
7. Personas, Habilidades y Competencias

2.3.4 Modelo de Referencia de Procesos de COBIT 5

COBIT 5 incluye un modelo de referencia de procesos que define y describe en detalle los procesos de Gobierno y de Gestión. Esto involucra todos los procesos respecto a las actividades de IT que se encuentra en una empresa, ofreciendo un modelo de referencia común entendible para gerentes de nivel operativo de TI y de negocio. El modelo de procesos propuesto es completo, exhaustivo, pero no es el único modelo posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación específica.

El modelo de referencia de procesos de COBIT 5 se subdivide en dos principales áreas, Gobierno y Gestión que a su vez cada una de estas contiene otros subprocesos (dominios):

- Gobierno. - Esta área contiene cinco procesos de Gobierno; dentro de cada proceso, se han definido prácticas de gobierno.
- Gestión. - Estos cuatro dominios están alineados con las áreas de responsabilidad de PBRM que proporcionan cobertura de TI extremo a extremo. Cada dominio contiene varios procesos, como en COBIT 4.1 y versiones anteriores.

El modelo de referencia de proceso de COBIT 5 es sucesor del modelo de proceso de COBIT 4.1, con los modelos de proceso de Risk IT y Val IT también integrados. En la siguiente figura (ver figura 6) muestra el conjunto completo de los 37 procesos de Gobierno y Gestión dentro de COBIT 5.

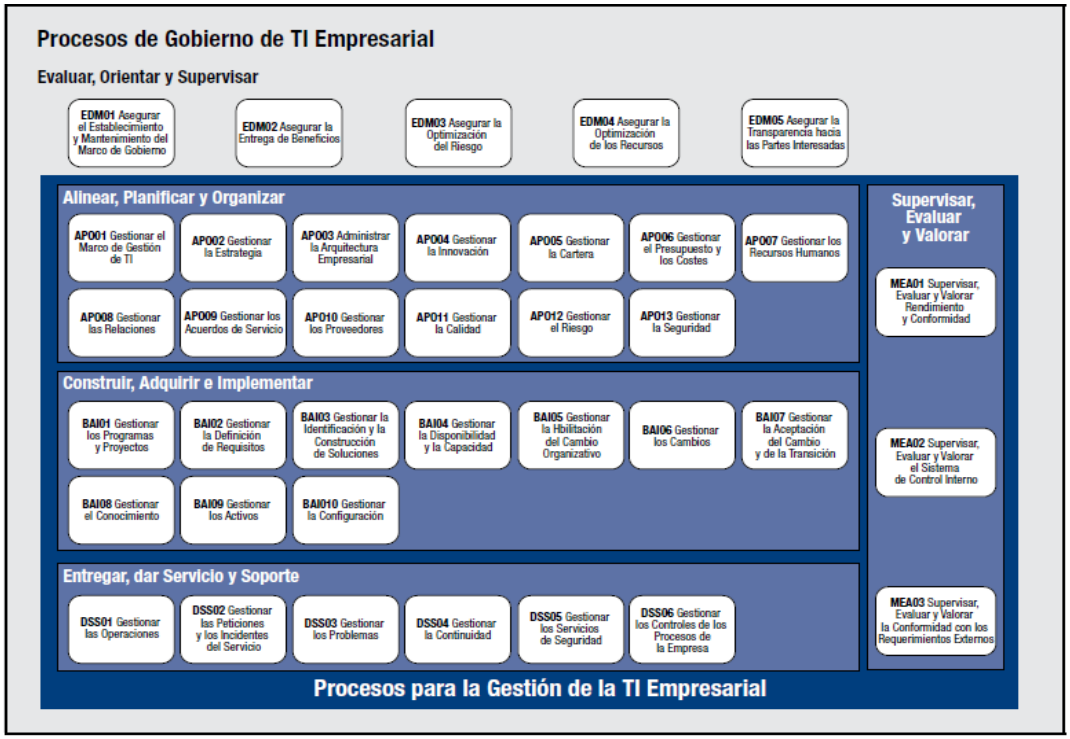

Figura 6. Modelo de Referencia de Procesos de COBIT 5
Fuente: (ISACA, Cobit 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, 2012)

2.3.5 Estructura de Procesos

La estructura de procesos de COBIT 5 es similar a la versión anterior, COBIT 4.1. Tras los cambios, se dispone de un total de 37 procesos (34 en la versión 4.1). COBIT 5 propone tres procesos para la monitorización y evaluación.

Seguramente en muchas organizaciones estos tres procesos están agrupados e implementados como un único proceso.

2.3.6 Características de COBIT 5

Una de las tantas características que dispone COBIT 5 es el incremento en la atención de la integración del negocio y TI. Esta orientación mejora la comunicación, clarifica los roles y responsabilidades y reduce los incidentes relacionados con la información y la tecnología que pueden dañar a la organización.

COBIT 5 integra las mejores prácticas dispersas en los distintos marcos de referencia de ISACA – COBIT, VAL IT, Risk IT, BMIS (Modelo de negocios para la seguridad de la información) e ITAF (Marco de referencia para el aseguramiento de TI) – en una sola base de conocimiento que permite tener un acercamiento consciente del valor, riesgo y seguridad en la organización.

2.4 Administración de Riesgos

La administración de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales, ayuda a identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso permitiendo a las organizaciones minimizar pérdidas y maximizar oportunidades.

2.4.1 Análisis de Riesgos

Es la etapa en la que se recopila la información acerca de la exposición de la operación al riesgo tecnológico, con el fin de tomar decisiones y

administrar los riesgos de forma apropiada. El análisis permite Identificar los riesgos, magnitud del riesgo y áreas que necesitan salvaguardas.

El análisis de riesgo aporta objetividad a los criterios en los que se apoya la seguridad, porque se centra en proteger los activos más críticos y permite a la organización gestionar los riesgos por sí misma. Este proceso debe estar perfectamente documentado para luego poder justificar las decisiones que se deben tomar (ver figura 7).

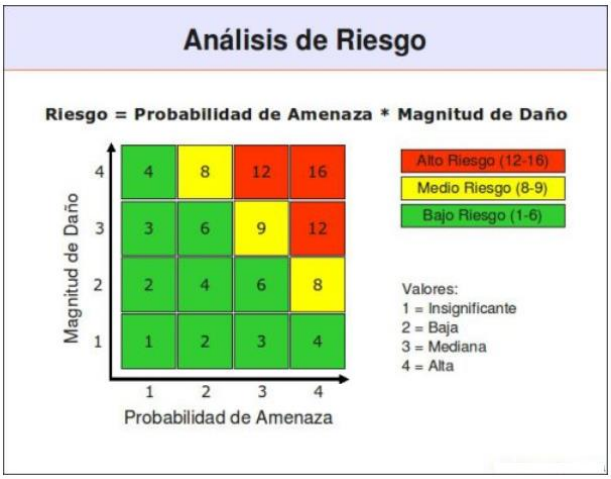

Figura 7. Análisis de Riesgo

Fuente: (Erb, 2012)

2.4.2 Proceso de Administración de Riesgos

La Administración de Riesgos es la que debe decidir qué nivel de riesgo está dispuesta aceptar, analiza el nivel tolerable que va aceptar para esto evaluará el costo beneficio, por esta razón las organizaciones deben ser conscientes de las vulnerabilidades, conocer los riesgos que enfrenta para establecer medidas correctivas y determinar responsabilidades desde un inicio.

Para que se pueda realizar la Administración de Riesgos, se requiere de un marco de referencia de las prácticas generalmente aceptadas de control y seguridad de Tecnología de Información con la finalidad de comparar el ambiente actual con el planeado.

La Administración de Riesgos determina los siguientes procesos que se detallan a continuación (ver figura 8):

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

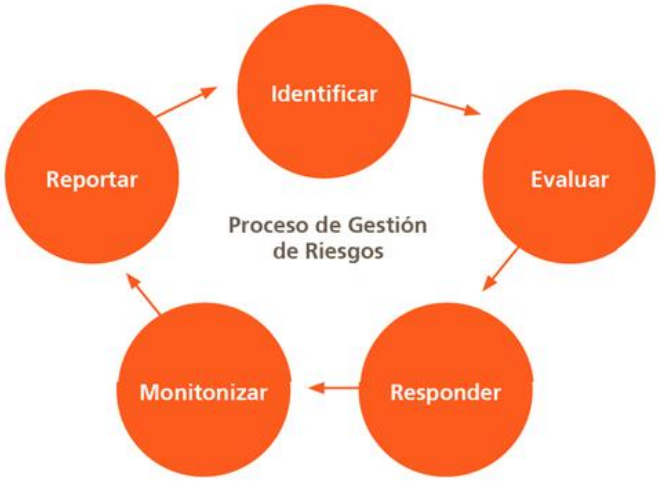

Figura 8. Procesos de Administración de Riesgos

Fuente: (ABENGOA)

La evaluación de riesgos y vulnerabilidades permite evaluar e identificar los riesgos operativos, haciendo énfasis en los activos de IT Físicos y lógicos, de esta forma se incluye una revisión física de las instalaciones y verificación de la seguridad de los elementos físicos y lógicos

Las empresas dependen cada vez más del funcionamiento de los sistemas de información para la ejecución de sus procesos comerciales y por lo tanto se encuentran expuestas a los riesgos informáticos que podrían incluir pérdida en la productividad, exposición de datos de los clientes y multas por violación de normas al conservar registros incorrectos, entre otros.

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

Existen varias metodologías de Gestión de riesgos como:

- Magerit
- ISO 27005
- Octave o Mehari

De forma general las metodologías contemplan los siguientes pasos:

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

Los métodos de análisis aplicados son:

- Cualitativo: clasificaciones descriptivas que describe impactos y probabilidades (Alto, Medio y Bajo)
- Semi cuantitativo: están asociados a una escala numérica
- Cuantitativo: utilizan valores numéricos para describir probabilidades de impacto

De acuerdo al tipo de riesgo se puede dar el siguiente tratamiento:

- Evitar: eliminando la actividad que causa el riesgo
- Mitigar: implementar controles para reducir la probabilidad e impacto.
- Transferir: pasar a otro la responsabilidad.
- Aceptar: asumir y monitorear.

Los beneficios de la administración de riesgos son:

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

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

2.5 Auditoría Informática

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

2.6 Marco Conceptual

COBIT 5.- Es un marco de referencia que proporciona buenas prácticas para cumplir los objetivos del negocio, alinea las metas estratégicas del negocio con las metas de TI, permite tener un ambiente de control para una correcta organización y administración de TI, brinda un aseguramiento razonable, previene, detecta o corre eventos no deseados. (ISACA, Cobit 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, 2012)

Información. - Es el activo fundamental en las empresas, representa la principal ventaja competitiva, proporciona apoyo a la alta dirección para la toma de decisiones, por lo que las empresas invierten grandes cantidades de dinero, tiempo y esfuerzo para crear sistemas que permitan administrar correctamente, obtener productividad y calidad. (ISACA, Cobit 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, 2012)

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

- Confidencialidad: Garantizar que información sensitiva sea vista por los accesos autorizados.
- Integridad: precisión y completitud de la información.
- Disponibilidad: Garantizar el acceso a la información y a los recursos relacionados cuando sea requerida por el negocio.

Auditoria de Sistemas de Información. - Proceso de recolección y evaluación de evidencia, para determinar que los sistemas de información cumplen los criterios de seguridad de la información, logran metas organizacionales y realizan un uso adecuado de los recursos. (ISACA, Cobit

5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, 2012)

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

Norma 410 de Tecnología de la información en Ecuador. - Se utiliza para control interno de entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos (Contraloría General del Estado, 2009).

2.7 Estado del Arte

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

- *La Universidad de EAFI en un boletín publicado en el año 2007,* hace énfasis en el uso de la herramienta COBIT para gestionar el proceso de auditoría de las compañías, también enfatiza que, si se aplica adecuadamente esta herramienta se puede evaluar de forma ágil y consistente el cumplimiento de controles detallados en una organización.

- *En América Latina existen* dos grupos de empresas: las que son reguladas y las que no lo son, en las no reguladas, alrededor del 80% de ellas no usan ningún estándar, el 20% restante que quieren mejorar, utilizan el estándar COBIT 5, que sería una opción muy buena para incentivar al porcentaje restante.

- *Sergio Sperat que es socio de Estratega y* tiene una trayectoria de más de 20 años como consultor en estrategia de áreas de TI y negocios, en una amplia variedad de industrias en Argentina, Chile, México y Estados Unidos, dice en uno de sus artículos sobre COBIT 5, que esta herramienta es la única que se ocupa de los controles específicos del área de TI desde una perspectiva del negocio, ya que permite alinear los objetivos del negocio con los de TI, porque se complementan, es decir van de la mano y se guían.

CAPÍTULO III
EJECUCIÓN DE LA AUDITORÍA

3.1 Dominio Evaluar, Orientar Y Supervisar.

En conformidad con el plan del proyecto para el Trabajo de Titulación, “Evaluación Técnica Informática de los procesos de Gobierno de TI a los Sistema de Información de la “ESPE” Sede Principal”, se realiza la revisión en base del Marco de Referencia COBIT 5, Dominio EDM (Evaluación, Orientación y Supervisión), de los procesos en el Sistema de Información de la “ESPE”, durante el período Enero – Diciembre del 2014.

3.1.1 Metodología

En el proceso metodológico de la Evaluación Técnica, se utiliza el marco de referencia de procesos COBIT 5 de ISACA, desde la definición de los aspectos de interés por medio de la cascada de metas, identificación de las necesidades de las partes interesadas de la institución, metas del negocio, metas de TI, con el uso de las plantillas propuestas por COBIT 5.

Una vez obtenidas y verificadas las metas con el personal involucrado, se determinan los procesos de Gobierno de TI, las prácticas de gestión y las actividades a ser evaluadas. Se prepara un Plan de Investigación de Campa, instrumentos de evaluación de campo y se ejecutan las técnicas de investigación formuladas de acuerdo al cronograma preparado, entre las técnicas se cuentan: entrevistas, cuestionarios y análisis documental de la información recibida.

3.1.2 Desarrollo de la Evaluación

Para el desarrollo de la Evaluación, se parte del Plan Estratégico (2014 - 2017), que dispone actualmente la ESPE, de este se toman los objetivos con la finalidad de alinearlos con las metas estandarizadas de negocio del marco de trabajo de COBIT 5, que representan las necesidades de las partes interesadas.

Alineación de las Metas del Negocio con las Metas de TI: Con el fin de garantizar que TI soporte las metas del negocio, se debe lograr su alineación, a fin de optimizar la inversión del negocio en TI y la administración en forma adecuada de los riesgos y oportunidades asociadas a TI.

Se valora la relación entre las metas del negocio y las metas de TI, para determinar cuáles son de mayor impacto y determinar Principales y Secundarios (ver anexo I).

Alineación de las metas de TI con los Procesos de Gobierno de TI: Las metas de TI que se ajustan a las necesidades de la UTIC, son adoptadas e identificadas de acuerdo a los procesos definidos en el marco de trabajo COBIT 5.

Para determinar e identificar las metas de TI con ponderaciones más altas se procede vincular con los procesos del Dominio de Evaluación, Orientación y Supervisión, en base a una valoración definida en cada una de las metas de TI con los procesos de Gobierno (ver cuadro 1).

Cuadro 1
Valorización de Procesos vs metas TI

DESCRIPCIÓN	Valor
Alto	3
Medio	2
Bajo	1

Se obtiene como resultado los procesos que serán evaluados como se indica (ver anexo II).

Así se determina los procesos que tienen mayor riesgo, que no permiten el cumplimiento de las metas corporativas, ni las prácticas de gestión al igual que las actividades relacionadas con los procesos.

Para analizar en detalle los procesos Evaluar, Orientar y Supervisar del dominio de Gobierno TI se considera:

- Descripción del proceso como un conjunto de prácticas influenciadas por las políticas de la organización.
- Declaración de Propósito.
- Objetivos vinculados a las TI que se determinan en la Matriz Objetivo vs Metas TI (ver anexo II).
- Cada objetivo vinculado a las TI y asociado a las métricas genéricas relacionadas.
- Objetivos del proceso.
- Cada objetivo del proceso está asociado a un conjunto de métricas genéricas.
- Cada proceso tiene un conjunto de Prácticas de Gobierno, estas prácticas son guías para alcanzar los objetivos, a continuación, se detalla en el siguiente cuadro el proceso como tal, con sus respectivas entradas y salida
- Cada Práctica de Gobierno tiene un conjunto de entradas y salidas que son necesarios para apoyar la funcionalidad del proceso. Como se puede observar en el siguiente cuadro (ver cuadro 2).

Cuadro 2
Entradas/Salidas de los Procesos

PRÁCTICA DE GOBIERNO				
DESCRIPCIÓN	**VIENE DESDE**	**ENTRADAS**	**SALIDAS**	**SALE A**
EDM01.01 Evaluar el sistema de Gobierno. Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del Gobierno de TI de la empresa.	MEA03.02	Comunicaciones de los requerimientos de cumplimiento modificados	Principios directrices del Gobierno de la empresa	EDM02
	Fuera del Ámbito de COBIT	- Tendencias en el entorno del negocio - Regulaciones - Gobierno/modelo de toma de decisiones - Constitución / normas / estatutos de la organización	Modelo de toma de decisiones	EDM02
			Niveles de autoridad	EDM02

Los procesos están asociados a una matriz genérica RACI, cada tarea, actividad o grupo de tareas es asignada a uno o más de los roles de la matriz RACI. Como ejemplo a continuación se detalla uno de los procesos con los respectivos responsables asignado para este caso (ver cuadro 3).

Cuadro 3
Matriz RACI

DESCRIPCIÓN	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de Negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Oficina de Gestión de Proyectos	Director de Gestión de Riesgos (CRO)	Director de la Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Comité de Riesgos Corporativos	Director de Recursos Humanos	Cumplimiento Normativo	Auditoría	Director de Informática (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio	Gestor de la Seguridad de la Información	Gestor de Continuidad de Negocio
EDM01.01. Evaluar el sistema de Gobierno	A	R	C	C	R		R				C		C	C	C	C	C	R	C	C	C				
EDM01.02. Orientar el sistema de Gobierno	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I
EDM01.03. Supervisar el sistema de Gobierno	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I

Cada práctica de Gobierno está asociada a un conjunto de actividades que determina COBIT 5 (ver anexo III).

En la reunión del 22 de abril del 2015 a las 8:00 am, en la UTIC de la ESPE, se acuerda entregarla información necesaria a los consultores para que puedan identificar y analizar las evidencias, sean estas físicas o digital.

Una vez identificadas las actividades ‘directrices para alcanzar prácticas de gestión para un gobierno y gestión de TI exitoso en la Institución’, se analiza cada una de estas con la finalidad de generar un cuestionario de 32 preguntas abiertas, que permitan evaluar la situación actual de la Institución (ver anexo V); este cuestionario fue dirigido al Director de la UTIC, quien delegó un funcionario para proporcionar información que evidencie las respuestas dela encuesta (ver anexo IV).

Esta información es clasificada y analizada según las actividades del proceso de Gobierno a evaluar. Se contrasta las respuestas obtenidas con la documentación recibida.

De acuerdo a lo encontrado en la evidencia proporcionada, el consultor emitió informe de observaciones y recomendaciones para cada uno de los procesos. Este informe está dirigido al Comité de Tecnología y al Rector de la institución como máxima autoridad, para mejorar de la continuidad de los servicios que proporciona la Universidad de las Fuerzas Armadas.

CAPÍTULO IV
INFORMEY RESULTADOS

4.1 Introducción.

Luego de revisar y analizar la documentación proporcionada por la Unidad de Tecnología, que utiliza la Universidad de las Fuerzas Armadas y de acuerdo al marco de referencia de COBIT, se pudieron obtener conclusiones que nos permitieron generar recomendaciones, las mismas que se encuentran en el presente Informe.

4.2 Resumen Ejecutivo.

El objetivo principal de la evaluación, es detectar si la gestión de la UTIC es la adecuada para cubrir todas las necesidades de la Universidad de las Fuerzas Armadas, Sede Principal.

La Evaluación se realizó en función de entrevistas y obtención de información, sostenidas con el personal técnico de la UTIC, donde se hizo el análisis y evaluación de las políticas, controles de aplicación y procedimientos de TI existentes.

El contenido de esta evaluación, está basada en el Dominio de Gobierno de TI (EDM) de COBIT 5 con sus respectivos procesos que son:

Evaluar, Orientar y Supervisar (EDM)

01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.

02. Asegurar la entrega de beneficios

03. Asegurar la optimización del riesgo

04. Asegurar la optimización de recursos

Se inició la evaluación realizando la investigación de los procesos que se consideran prioritarios para la Institución, considerando su funcionamiento e importancia, además se evaluó los posibles riesgos que se han presentado.

Para lo cual en un futuro inmediato se recomienda formular, ejecutar y evaluar un Plan de mejora por parte de la alta gerencia y dar cumplimiento a las recomendaciones emitidas en el Informe Detallado de la Evaluación Técnica Informática, los informes especiales y la Matriz de Correlación de COBIT 5 realizadas por el evaluador.

4.3 Descripción del Trabajo Efectuado.

Una vez analizada y conocida la situación actual de la Institución y definido el enfoque de la evaluación a ser utilizado, así como los responsables del negocio y de la parte tecnológica; se realizarán las siguientes actividades:

- Detallar la manera en que se comprobará cada una de las actividades de control, señaladas en el enfoque de auditoría, tanto en su implementación, como en su eficacia operativa.
- Determinar la documentación necesaria, para probar cada actividad de control e identificada en el dominio de Gobierno de TI (EDM).
- Planificar, cuestionarios y entrevistas con los encargados de la Unidad de Tecnología de la Universidad de las Fuerzas Armadas, con la finalidad de conocer más a detalle los procesos y procedimientos existentes en la entidad y solicitarla documentación existente.
- Una vez obtenida la información, realizar su respectivo análisis y documentación, en concordancia con el primer punto, esto con la finalidad de emitir una conclusión para cada actividad de control.
- Una vez analizados los atributos de control de cada actividad, emitir una conclusión acerca de la implementación y de la eficacia.
- Diseñar y elaborar el informe de auditoría, donde por cada Objetivo de Control se detallará:
    - Observación
    - Criterio
    - Condición
    - Causa
    - Efecto
    - Recomendaciones

- Emitir el informe final de auditoría, en el cual se detalla todas las oportunidades de mejora encontradas y sus respectivas recomendaciones emitidas.

4.4 Informe Detallado.

4.4.1 Antecedentes

La Universidad de las Fuerzas Armadas, desde hace algunos años, ha venido ejecutando varios proyectos relacionados con el área de TI, con el objeto de apoyar a las diferentes actividades que realiza la Institución; por lo que esta vez, ha solicitado a través de la Unidad de Desarrollo Institucional, elaborar un proyecto para obtener información adecuada y pertinente acerca del desempeño de la Unidad de Tecnología de la Información de la ESPE y de su Sistema de Información Institucional con la finalidad de mejorar cada uno de los procesos existentes.

Por tal razón fue necesario realizar una Evaluación Técnica en base a los lineamientos del Marco de Referencia COBIT 5.0, estos resultados serán proporcionados a la alta gerencia, mediante un informe final oportuno y veraz para la toma de decisiones.

4.4.2 Objetivo

Realizar una Evaluación Técnica Informática de los Procesos de Gobierno de TI, en la Universidad de las Fuerzas Armadas “ESPE” Sede Principal, mediante la revisión del ambiente de control, implementado en los procesos automatizados y en el gerenciamiento de los mismos, utilizando COBIT 5, a fin de identificar debilidades y emitir recomendaciones que permitan minimizar los riesgos.

4.4.3 Alcance de la Evaluación Técnica.

El presente proyecto está orientado a la evaluación y revisión del control interno de los procesos de Gobierno de TI, para esto se realizó, la identificación de los requerimientos de información relevantes del negocio, lo que permitió realizar la selección de los procesos y actividades utilizando

COBIT 5, posteriormente se elaboró un Plan de Investigación de Campo o Programa de Auditoría, con el que se recopiló la información pertinente y las evidencias necesarias.

4.4.4 Resultados de la Evaluación Técnica.

4.4.4.1 EDM01.Asegurar el Establecimiento y Mantenimiento del Marco de Referencia de Gobierno

EDM01.01: Evaluar el Sistema de Gobierno.

Observación EDM01.01: No existe evidencia que en la Universidad de las fuerzas Armadas ESPE se disponga de lineamientos, normas y procedimientos que permitan realizar una evaluación periódica de su Sistema de Información.

Criterio:

- (ISACA, COBIT 5 Procesos Catalizadores, 2014): Con el fin de evaluar el Sistema de Información se deberá “Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del Gobierno de TI de la empresa” (ISACA, 2012).

- NTI-CGE-Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, (410-04) Políticas y Procedimientos: La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

  La unidad de tecnología de información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran (Contraloría General del Estado, 2009).

Condición:

La ESPE tiene un Catálogo de Servicios, elaborado por la Unidad de Tecnología de la Información y Comunicación UTIC, donde se indica los servicios que presta actualmente la Institución a la Comunidad Universitaria, pero no existe evidencia de que sean evaluados periódicamente para medir el grado de capacidad de los servicios (Evidencia Nro.2014-0483-ESPE-d-6 Catálogos de Servicios 2011-2013").

Causa:

- No existe evidencia de la existencia de un Comité de Tecnología en la Institución.
- No existe evidencia de un "Catálogo de Servicios" actualizado.
- No existe evidencia de que la ESPE disponga de políticas para la evaluación y monitoreo del Sistema de Información de la ESPE.
- El diseño organizacional no contempla estas funciones, ni asigna estas responsabilidades a una Unidad específica.

Efecto:

- La evaluación inadecuada al Sistema de Información, afecta la calidad de los servicios de TI ofrecidos y su mejoramiento, no se tiene conciencia de la inversión necesaria ni de la relación del cumplimiento de los objetivos institucionales.

Riesgo Alto.

Recomendación:

- El Señor Rector, durante el segundo semestre del año en curso, dispondrá el trámite correspondiente para la creación del Comité de Tecnología de la Institución, en conformidad con las buenas prácticas de tecnología de COBIT 5 y las NTI-CGE.

- El Comité de Tecnología, una vez creado y de forma inmediata, diseñará y pondrá en ejecución un proceso participativo para establecer lineamientos, políticas y procedimientos que permitan evaluar el desempeño del Sistema de Información de la ESPE y brindar servicios de calidad.

- El Director de la UTIC, hasta el segundo semestre del año en curso, dispondrá la actualización del catálogo de servicios de TI en conformidad con el marco de referencia COBIT 5 y las NTI-CGE.

- El Comité de Tecnología, una vez actualizado el Catálogo de Servicios de TI, dispondrá la evaluación del mismo en conformidad con el marco de referencia COBIT 5 y las NTI-CGE, esta evaluación deberá ser ejecutada periódicamente para medir el grado de eficiencia y eficacia del Sistema de Información que dispone la Universidad de las Fuerzas Armadas ESPE.

EDM01.02: Orientar el Sistema de Gobierno.

Observación EDM01.02: No existe ninguna evidencia de que la Institución disponga de un plan de difusión que permita garantizar que los mecanismos de notificación utilizados proporcionen información adecuada a aquellas personas que tienen la responsabilidad de la supervisión y toma de decisiones sobre los principios de Gobierno de TI.

Criterio:

- ISACA, COBIT 5 Procesos Catalizadores, 2014: Expone como criterio, “Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el Gobierno de TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el Gobierno. Definir la información necesaria para una toma de decisiones informadas “ (ISACA, 2012).

- NTI-CGE-Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, (410-02) Políticas y Procedimientos: La Unidad de tecnología de información deberá promover y establecer convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, así como de programas de aplicación desarrollados al interior de las instituciones o prestación de servicios relacionados con la tecnología de información (Contraloría General del Estado, 2009).

Condición:

- En la actualidad la Institución no dispone de un plan de difusión que permite mantener informado a la alta gerencia de la ESPE, sobre la situación actual del Sistema de Información de la Universidad. Esta falta de comunicación a las autoridades da como resultado que el apoyo por parte de ellos, sea limitado o inclusivo nulo a las gestiones internas que lleva la UTIC; lo que conlleva tomar decisiones correctas y a tiempo por parte de la máxima autoridad.

Causa:

- Falta de un plan de difusión donde se incluya procedimientos y normas, que permita mantener informado sobre la situación actual de los procesos que se están ejecutando diariamente en la UTIC.
- Desconocimiento del encargado de promulgar las normativas a la Comunidad Universitaria.

Efecto:

- La falta de socialización de los procedimientos y normas, no permite tomar medidas correctivas por parte de las autoridades.
- La falta de un adecuado canal de comunicación entre los involucrados, hace que los servicios que presta UTIC a la Comunidad Universitaria no sean los adecuados, debido a la forma como se están llevando internamente los procesos sin ser socializados.

Riesgo Alto.

Recomendación:

- El Comité de Tecnología, una vez creado y de forma inmediata, elaborará un plan que permitirá orientar a alta gerencia sobre la guía de las estructuras, directrices y principios de gobierno de TI a seguir, con el fin de tener información necesaria para la toma de decisiones.
- Una vez generado el plan de comunicación por el Comité de Tecnología, este deberá ser entregado al Director de la UTIC para que ponga en ejecución en un plazo máximo de seis meses del año en curso, de acuerdo al marco de referencia COBIT 5 y las NTI-CGE. Este plan debería ser evaluado periódicamente por la Institución con la finalidad de medir el nivel de capacidad de cada uno de los procesos.

EDM01.03: Supervisar el Sistema de Gobierno.

Observación EDM01.03: No existe evidencia alguna que permita analizar que las prácticas de monitoreo existentes, sean las más adecuadas para la supervisión de los servicios de información de la Institución.

Criterio:

- ISACA, COBIT 5 Procesos Catalizadores, 2014: Expone como criterio, “Supervisar la ejecución y la efectividad del Gobierno de TI de la empresa. Analizar si el sistema de Gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI” (ISACA, 2012).

- De acuerdo a la Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, (410-02): La unidad de tecnología de la información elaborará e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y éste con el Plan Nacional de Desarrollo y las políticas públicas de gobierno (Contraloría General del Estado, 2009).

Condición:

Actualmente la UTIC, no dispone de lineamientos, normas y procedimientos que permita realizar la supervisión y monitoreo continuo de los procesos que se encuentran ejecutando diariamente y de esta forma medir el nivel de capacidad de cada uno de los procesos.

Causa:

La falta de mecanismos rutinarios y regulares de supervisión que permita evaluar el Sistema de Información, a pesar de que los responsables de los procesos se reúnen para analizar cuál es la situación actual de los recursos (HW, SW y RRHH) que administra la UTIC.

Efecto:

- Sin una adecuada supervisión no se puede determinar que los procesos de TI, estén alineados con los objetivos de la Institución.
- Si no se dispone de un plan de supervisión actualizado, esto impide la actualización tecnológica y resta competitividad a la institución.

Riesgo Medio.

Recomendación:

- El Comité de Tecnología una vez creado, deberá delegar una comisión responsable para el análisis y creación de un plan de supervisión aplicando el marco de trabajo de COBIT y las NTI-CGE, que permita evaluar la efectividad y determinar las acciones a tomar para rectificar cualquier falencia.

- El Director de la UTIC de la Universidad de las Fuerzas Armadas, una vez creado el plan de supervisión (lineamientos, políticas y procedimientos), deberá socializar a todo el personal en general, hasta el segundo semestre del año en curso, las directrices necesarias para la ejecución e implementación de este plan, lo que permitirá evaluar el desempeño de los servicios que presta la Institución.

4.4.4.2 EDM02. Asegurar la Entrega de Beneficios

EDM02.01: Evaluar la Optimización de Valor.

Observación EDM02.01: No existe evidencia que permita verificar que existan procedimientos de evaluación continua de los servicios y activos del portafolio de TI, que aseguren la entrega de beneficios a un costo razonable y permita la optimización de valor para la Institución.

Criterio:

ISACA, COBIT 5 Procesos Catalizadores, 2014: Expone como criterio, "Evaluar continuamente las inversiones, servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa y aportar valor a un coste razonable. Identificar y juzgar cualquier cambio en la dirección que necesita ser dada la Gestión para optimizar la creación de valor". (ISACA, 2012)

Condición:

Actualmente no se puede medir la optimización de valor, ya que no existe un plan de gestión de servicios actualizado que permita cumplir con el alcance de objetivos; además la Institución mediante la aprobación del Reglamento Orgánico de Gestión Organizacional por Procesos (ESPE HCUP-RES-2014-144), podrá en el futuro identificar y juzgar los cambios necesarios en base a procedimientos establecidos.

Causa:

- Desconocimiento de la situación actual de la operatividad de los Sistemas de Información que administra la UTIC.
- Falta de presupuesto para realizar la evaluación de las inversiones, servicios y activos del portafolio de TI.

Efecto:

- No se puede alcanzar los objetivos planteados por la Institución a un costo razonable.

- Disminución en el acceso a los recursos Tecnológicos que proporciona la Universidad.

Riesgo Medio.

Recomendación:

- Una vez creado el Comité de Tecnología, dentro de una de sus funcionalidades deberá ser el encargado de evaluar periódicamente la efectividad de la integración y del alineamiento de las estrategias de TI con los objetivos de la Institución para aporta valor.

- El Director de la UTIC, deberá analizar, comprender y evaluar semestralmente las inversiones, servicios y activos de TI que actualmente está prestando la Institución, así como los roles, responsabilidades, asignaciones y organismos de toma de decisiones existentes, para asegurar la creación del valor; esto permitirá mejorar continuamente cada uno de los procesos involucrados.

EDM02.02: Orientar la Optimización del Valor.

Observación EDM02.02: No existe evidencia de que la ESPE haya socializado algún plan para gestionar los procesos a los usuarios, con el fin de impulsar el incremento de valor para la Institución.

Criterio:

ISACA, COBIT 5 Procesos Catalizadores, 2014: Expone como criterio, “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” (ISACA, 2012).

Condición:

Actualmente la Institución no dispone de un plan de comunicación actualizado sobre los procesos que están llevando a cabo; este plan debe

contener lineamientos, políticas y procedimientos que están orientados a la optimización del valor.

Causa:

Falta de lineamientos a nivel de directorio para establecer procesos, normas y procedimientos para la correcta ejecución de un plan de gestión de procesos.

Efecto:

- Desorden en las diferentes actividades que se ejecutan dentro de UTIC.
- Bajo desempeño del departamento UTIC.

Riesgo Medio.

Recomendación:

- El Comité de Tecnología una vez creado, deberá delegar a los responsables para analizar los cambios necesarios en la asignación de imputaciones y responsabilidades para la ejecución del portafolio de inversiones y la entrega de valor a partir de los servicios que actualmente está prestando la Institución.
- El Director de la UTIC, durante el segundo semestre del año en curso, deberá definir los principios, procedimientos y prácticas de Gestión de valor, a los responsables necesarios para dar seguimiento que permitan optimizar los recursos y servicios de Gobierno TI y obtener un coste/beneficio para la Institución.

EDM02.03: Supervisar la Optimización de Valor.

Observación EDM02.03: Actualmente la Universidad de las Fuerzas Armadas, no dispone de normas, directrices y lineamientos que permitan medir el grado de valor que está generando para determinar con exactitud el desempeño de los servicios que ofrece a la Comunidad Universitaria.

Criterio:

ISACA, COBIT 5 Procesos Catalizadores, 2014: Expone como criterio, “Supervisar los indicadores clave y sus métricas para determinar el grado en que el negocio está generando el valor y los beneficios previstos de los servicios e inversiones TI. Identificar los problemas significativos y considerar las acciones correctivas”. (ISACA, 2012)

Condición:

La UTIC, sin la disponibilidad de un plan actualizado de procesos donde se indique la correcta aplicación de indicadores y métricas no puede realizar la supervisión adecuada que permita generar valor y por lo tanto no se dispone de informes que indique cuál es la situación.

Causa:

La UTIC, no acoge completamente la NTI-CGE-Norma 410 TECNOLOGÍA DE LA INFORMACIÓN establecida, por la Contraloría General del Estado, donde se indica los lineamientos que se debe aplicar para la correcta supervisión.

Efecto:

- Datos no confiables, sobre la medición de rendimiento de los servicios proporcionados por UTIC.
- Sin un monitoreo eficiente de los servicios de TI, no se puede identificar los problemas más significativos que se presentan a diario y poder tomar acciones correctivas de inmediato.

Riesgo Medio.

Recomendación:

- El Comité de Tecnología una vez creado, deberá solicitar los informes habituales, existentes y relevantes de la funcionalidad de los servicios de TI en la Institución, con la finalidad de analizar y conocer cuál es la situación actual para que se informe a alta gerencia y esta pueda tomar

decisiones apropiadas según sea necesario para asegurar que el valor sea optimizado.

- El Director de la UTIC deberá asegurar a corto plazo, que la medición y elaboración de los informes en cuanto a conformidad y desempeño de las TI de la Institución sean oportunos, completos, fiables transparentes y precisos para informar sobre los avances de la entrega de valor, respecto a los objetivos trazados, lo que permitirá asegurar que los resultados esperados se estén logrando.

4.4.4.3 EDM03. Asegurar la Optimización del Riesgo

EDM03.01: Evaluar la Gestión de Riesgos.

Observación EDM03.1:

- No existe evidencia de un análisis de riesgos actual, que permita identificar y valorar los nuevos riesgos de TI a los que se encuentra expuesta la Universidad de las Fuerzas Armadas ESPE.
- No existe evidencia que permita conocer el apetito de riesgo de TI, que la Universidad de las Fuerzas Armadas ESPE pueda aceptar, y/o tolerar.

Criterio:

ISACA, COBIT 5 Procesos Catalizadores, 2014: expone como criterio: “Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado” (ISACA, 2012).

Condición:

Según documento electrónico “PLAN_DE_CONTINGENCIA” se constata que el último análisis de riesgo realizado a la Universidad de las Fuerzas Armadas ESPE fue en el año 2011, por tal razón no se tiene un análisis de riesgo actual.

Causa:

- No hay política permanente que defina la realización de un análisis de riesgo.

Efecto:

- No se cuenta con un análisis de riesgo de la situación actual de TI.
- Bases de proyectos Tecnológicos sobre análisis de riesgo desactualizados.
- Falta de cumplimiento de la NTI-CGE-Norma 410 TECNOLOGÍA DE LA INFORMACIÓN, (410-11).
- Por la falta de un plan de gestión de riesgos actualizado, no se permite salvaguardar los activos actuales y futuros de TI en su totalidad.
- Desconocimiento del nivel de riesgos de TI, que la Universidad de las Fuerzas Armadas ESPE estaría dispuesta a asumir, o tolerar.

Riesgo Alto.

Recomendación:

- El Director de la UTIC, de manera inmediata, dispondrá el trámite correspondiente para la ejecución de la Evaluación de Gestión de Riesgos a realizarse a nivel de las TI en la Universidad de las Fuerzas Armadas ESPE.
- Esta evaluación de Riesgo, debe ser documentada, revisada y actualizada periódicamente en base a estándares nacionales e internaciones, así como las decisiones que se tomen deben ser en base a un apetito de riesgo vigente.

EDM03.02: Orientar la Gestión de Riesgos.

Observación EDM03.02: No existe evidencia de cultura de riesgos TI, que permita identificar estrategias vigentes de riesgos de TI dentro de la Universidad de las Fuerzas Armadas ESPE.

Criterio:

ISACA, COBIT 5 Procesos Catalizadores, 2014: expone como criterio, “Orientar el establecimiento de prácticas de Gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual, no excede el apetito de riesgo del Consejo” (ISACA, 2012).

Condición:

- Según el resultado de la evidencia “Encuesta No 1” y revisión de la documentación entregada no se constata ningún documento que respalde los mecanismos de comunicación de riesgos a todos los niveles de la Universidad de las Fuerzas Armadas ESPE.
- Según documentos electrónicos recibidos, no se visualizan planes de acción de riesgos.

Causa:

- No cumple con la norma de control interno de la Contraloría General del Estado 410-10: Seguridad de tecnología de información, numeral 5 donde indica que “Se deben realizar monitoreo, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados”.
- No cumple con la norma de control interno de la Contraloría General del Estado 410-11 Plan de contingencias, numeral 2 que menciona que “El plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización”.
- No cumple con la norma de control interno de la Contraloría General del Estado 410-11: Plan de contingencias, numeral 7 donde indica que: “El plan de contingencias aprobado, será difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas, o cuando se haya efectuado

algún cambio en la configuración de los equipos o el esquema de procesamiento".

Efecto:

- No se cuenta con planes de acción de Riesgos a implementarse ante la materialización de una amenaza,
- Pérdida de la disponibilidad del Sistema de Información que administra la UTIC en la Universidad de las Fuerzas Armadas ESPE.

Riesgo Alto.

Recomendación:

- El Comité de Tecnología una vez creado deberá promover una cultura de riesgos TI a lo largo de Universidad de las Fuerzas Armadas ESPE, que permita identificar los riesgos TI, oportunidades e impactos a los que se puede estar expuestos, como Institución, verificando que no se exceda el apetito del riesgo.
- El Comité de Tecnología una vez creado durante el segundo semestre del año en curso, dispondrá el trámite correspondiente para ejecutar un plan de comunicación de riesgos cubriendo todos los niveles de la organización y planes de acción de riesgo.

EDM03.03: Supervisar la Gestión de Riesgos.

Observación EDM03.03: No existe evidencia que supervise la gestión de riesgos dentro de la UTIC, provocando ausencia de resultados de análisis e informes de riesgos, y/o acciones correctivas a las partes interesadas.

Criterio:

ISACA, COBIT 5 Procesos Catalizadores, 2014: expone como criterio, "Supervisar los objetivos y las métricas clave de los procesos de Gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución" (ISACA, 2012).

Condición:

Según la evidencia documental entregada por UTIC, no se encuentra respaldo digital, tampoco se ha recibido documentación física, que permita abalizar la realización de resultados de evaluaciones de riesgos, medidas de acciones correctivas, identificación de problemas y solución de los mismos.

Causa:

- No cumple con la norma de control interno de la Contraloría General del Estado 410-11 Plan de contingencias, numeral 2 que menciona que “El plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización”.
- No se corroboran en que las acciones a ejecutarse ante una contingencia sean las más óptimas y permitan la continuidad de los servicios del Sistema Informático que administra la UTIC, por cuanto el análisis de riesgo es obsoleto.

Efecto:

- No se conoce si los riesgos TI que existen, puedan pasar los límites del apetito de riesgo.
- Las partes interesadas no tienen la certeza que se cumplan con los objetivos de la Universidad de las Fuerzas Armadas ESPE.
- Pérdida total de disponibilidad y demora en la recuperación de los servicios de TI.

Riesgo Alto.

Recomendación:

- El Director de la UTIC de manera inmediata debe disponer la creación de métricas de riesgos que permitan conocer de manera mensual los diferentes incidentes o problemas que se pueden presentar y amenazan

la disponibilidad de los Sistemas de Información, el tiempo de respuesta ante los incidentes y la frecuencia con que se repiten.

- El Comité de Tecnología una vez creado, durante el segundo semestre del año en curso, dispondrá el trámite correspondiente para la ejecución y verificación del Plan de Pruebas, con el fin de verificar que mejoras, y/o cambios se deben considerar.

4.4.4.4 EDM04. Asegurar la Optimización de Recursos

EDM04.01: Evaluar la Gestión de Recursos.

Observación EDM04.01: No se ha realizado el levantamiento de la arquitectura empresarial tecnológica en la UTIC de la Universidad de las Fuerzas Armadas ESPE. Se evidencia en la Encuesta 01.

Criterio:

ISACA, COBIT 5 Procesos Catalizadores, 2014: expone como criterio, “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”. (ISACA, 2012)

Condición:

Según el resultado de la evidencia “Encuesta No 1”, no se ha realizado levantamiento de la arquitectura empresarial tecnológica, no es posible realizar un adecuado aprovisionamiento de recursos TI. Se corre el riesgo de realizar inversiones de recursos TI innecesarias o insuficientes teniendo como resultado final un servicio de muy baja calidad.

Causa:

- No hay política que defina la realización de un Plan de Recursos que permita entregar valor y la mitigación del riesgo de los recursos asignados.

Efecto:

- Desconocimiento de la Infraestructura Tecnológica (Hardware, Software, y Comunicaciones) con los que cuenta la Universidad de las Fuerzas Armadas.
- No se puede determinar cuál es la situación actual y en qué condiciones se encuentran los recursos de TI, para tomar medidas necesarias que permitan el mejoramiento de la infraestructura tecnológica.

Riesgo Alto.

Recomendación:

- El Comité de Tecnología una vez creado, durante el segundo semestre del año en curso, deberá disponer a la alta gerencia la creación de un plan estratégico de recursos TI, que permita gestionar los recursos asignados a cada uno de los usuarios de acuerdo a las prioridades y limitaciones presupuestarias.
- El Director de la UTIC una vez que disponga del plan de Recursos, de manera inmediata deberá evaluar y gestionar el aprovisionamiento de Recursos de TI de forma precisa y objetiva.
- Una vez definido las necesidades de los usuarios, el Director de UTIC deberá argumentar mediante un plan estratégico de recursos TI, la asignación de recursos económicos que permitan solventar estas necesidades de la Institución.

EDM04.02: Orientar la Gestión de Recursos.

Observación EDM04.02: No existe evidencia que permita determinar cuáles son las medidas y métricas para la gestión de los recursos, al igual que los principios que permita proteger los diferentes recursos TI; tampoco se conoce las causas frecuentes, por las cuales se solicita los servicios del personal de TI.

Criterio:

ISACA, COBIT 5 Procesos Catalizadores, 2014: expone como criterio, “Asegurar la adopción de principios de Gestión de recursos para permitir un uso óptimo de los recursos de TI a lo largo de su completo ciclo de vida económica” (ISACA, 2012).

Condición:

Según el resultado de la evidencia “Encuesta No 1”, la Planificación de recursos de TI es obsoleta lo cual no permite definir objetivos, medidas y métricas de la gestión de los recursos.

Causa:

- Falta de cumplimiento de las estrategias de arquitectura en la UTIC.
- Falta de comunicación de estrategias de reasignación de recursos TI.
- Falta de planificación del Personal Humano y financiero de la UTIC.

Efecto:

- Al no disponer de un plan de estrategias y principios de recursos TI, la UTIC no puede medir las brechas existentes y realizar los cambios necesarios para cumplir con los objetivos trazados por la Institución.
- Al carecer de un plan de infraestructura tecnológica no se puede argumentar la necesidad y la importancia de invertir en ella y por ende que se le asigne el presupuesto necesario.

Riesgo Alto.

Recomendación:

- El Comité Tecnológico una vez creado, durante el segundo semestre del año en curso, deberá establecer mecanismos para la implementación de un plan de capacitación que permita optimizar recursos TI y gestionar la disponibilidad de los mismos, este plan debe ser socializado con el fin de satisfacer las necesidades de los usuarios.

- Luego de disponer del Plan de Capacitación sobre la optimización de recursos, es necesario que el Director de la UTIC defina los lineamientos y normas que debe seguir todo el personal involucrado para el cumplimiento de los objetivos trazados por la Institución.

EDM04.03: Supervisar la Gestión de Recursos.

Observación EDM 04.03: No existe un plan que supervise la gestión de recursos que administra la UTIC, esto no permite determinar la asignación y optimización de recursos asignados a cada uno de los usuarios de la Institución.

Criterio:

ISACA, COBIT 5 Procesos Catalizadores, 2014: expone como criterio, “Supervisar los objetivos y métricas clave de los procesos de Gestión de recursos y establecer cómo serán identificados, seguidos e informados para su resolución las desviaciones o los problemas” (ISACA, 2012).

Condición:

De la encuesta realizada “Encuesta Nº 1” se determina que no existe un documento que respalde, el análisis de la asignación y optimización de recursos de acuerdo con las prioridades de la Institución, para evaluar las condiciones por las cuales se debería hacer reposiciones de los recursos de TI.

Causa:

- No hay política para la ejecución de un Plan de Supervisión de recursos.

Efecto:

- No se puede generar estrategias de aprovisionamiento de recursos TI, por no contar con una bitácora de incidentes en la infraestructura tecnológica.
- No se puede tomar acciones correctivas inmediatas que permitan hacer frente a las desviaciones de gestión de recursos.

- Demora en la operatividad y disponibilidad de los recursos de TI.

Riesgo Alto.

Recomendación:

- El Comité Tecnológico de TI una vez creado, durante el segundo semestre del año en curso, deberá disponer el trámite correspondiente para la creación de un plan de supervisión de recursos TI, el mismo que deberá contener en forma detallada reglas, normas y principios que permita supervisar todos los recursos TI con los que cuenta la Institución.
- El Director de la UTIC, una vez que disponga el plan de supervisión inmediatamente, deberá socializar y capacitar este plan a todo el personal involucrado para que garanticen la correcta utilización de los recursos TI, de manera que proporcionen valor a la Institución.

4.4.5 Resultados Obtenidos

Autovaloración de los Procesos

El análisis de madurez realizado a los procesos se sustenta con evidencias. Las calificaciones obtenidas obedecen a un promedio de porcentajes de cumplimiento de los objetivos de cada proceso; los porcentajes se otorgan en función de una apreciación de la cantidad de eventos que ocurren para alcanzar los objetivos.

A continuación, se presenta las matrices de cumplimiento de los objetivos de cada proceso (ver cuadro 4, 5, 6, 7).

Cuadro 4
Autoevaluación EDM01. Asegurar el establecimiento y mantenimiento del marco de referencia de Gobierno

EDM01.			
Propósito: Cumplir con los requisitos de la empresa de mantener o ampliar su estrategia de negocio y Gobierno mientras existe una transparencia sobre los beneficios, costos y riesgos.			
Meta del Proceso	**Metas Relacionadas**	**Cumple**	**Comentarios**
EDM01-01. 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	• Tiempo de ciclo actual vs objetivo para las decisiones clave • Nivel de satisfacción mediante encuestas a las personas interesadas	20% 10%	Las decisiones clave no pasan a un consejo para que se evalúen y luego se apruebe
EDM01-02. Garantizar que el sistema de Gobierno para TI está incorporado al Gobierno corporativo.	• Número de roles, responsabilidades y autoridades que están definidas, asignadas y aceptadas a gestores para una Gestión del negocio y de las TI apropiados. • Grado en que los principios de Gobierno acordados para las TI están evidenciados en procesos y prácticas (porcentaje de procesos y prácticas con clara trazabilidad a los principios) • Número de casos de no-cumplimiento con las directrices de comportamiento ético y profesional	30% 0% 40%	Están definidas las autoridades para la Gestión, pero no hay una comunicación adecuada entre ellos. Se ha dado casos esporádicos, y se ha manejado con llamados de atención
EDM01-03. Obtener garantías de que el sistema de Gobierno para TI está operando de manera efectiva	• Frecuencia de revisiones independientes del Gobierno de TI • Frecuencia del reporte del Gobierno de TI al Comité Ejecutivo y a la dirección • Número de aspectos de Gobierno de TI notificados	0% 0% 0%	A los directores no se da un reporte anual

Cuadro 5
Autoevaluación EDM02. Asegurar la entrega de Beneficios

EDM02.			
Propósito: Cumplir con los requisitos de la empresa de ser ágil para responder a cualquier requisito; proporcionar información consistente, confiable y aplicaciones sin problemas de integración en los procesos empresariales.			
Meta del Proceso	**Metas Relacionadas**	**Cumple**	**Comentarios**
EDM02-01. La empresa está asegurando un valor óptimo de su portafolio de iniciativas TI, servicios y activos aprobados.	• Nivel de satisfacción de la Gestión ejecutiva con la entrega de valor y los costes de TI	30%	El nivel de satisfacción es medio bajo debido al presupuesto asignado a TI.
	• Desviación entre la combinación objetivo e inversión actual	60%	Se cumple con el presupuesto planteado al inicio del año.
	• Nivel de satisfacción de las partes interesadas con la habilidad de la empresa para obtener valor de las iniciativas TI	40%	Se manifiesta una satisfacción media al asignar un prepuesto propio a TI.
EDM02-02. Se deriva un valor óptimo de la inversión TI mediante prácticas de Gestión del valor en la empresa.	• Número de incidentes que ocurren debido a la actual o tentativa evasión de los principios y prácticas de Gestión del valor establecidos	20%	Cuando no se toma en cuenta oportunamente a TI no se cumple con los plazos establecidos.
	• Porcentaje de iniciativas TI en el portafolio general en las que el valor está siendo gestionado a través del ciclo de vida completo	40%	No se cuenta a TI en la realización del plan estratégico
EDM02-03. Las inversiones individuales en TI contribuyen a un valor óptimo.	• Nivel de satisfacción de las partes interesadas basado en entrevistas con el progreso hacia las metas identificadas con el valor obtenido	30%	El nivel de satisfacción de las partes interesadas es regular según el cuestionario realizado.
	• Porcentaje del valor esperado realizado	40%	El valor de inversión que genera TI es a nivel de servicios para la comunidad Universitaria

Cuadro 6
Autoevaluación EDM03. Asegurar la Optimización del Riesgo

EDM03.			
Propósito: Cumplir con los requisitos de la empresa de tener estables, rentables, integrados y estandarizados los sistemas de aplicación, recursos y capacidades que cumplen con los requisitos actuales y futuros de la empresa.			
Meta del Proceso	**Metas Relacionadas**	**Cumple**	**Comentarios**
EDM03-01. Los umbrales de riesgo son definidos y comunicados y los riesgos clave relacionados con la TI son conocidos.	• Nivel de alineamiento entre riesgo TI y riesgo de negocio. • Número de potenciales riesgos TI identificados y gestionados. • Frecuencia de refresco de la evaluación de los factores de riesgo	30% 15% 20%	El negocio es la educación por lo que los riesgos que conciernen a los sistemas están alineados con el negocio. Se ha gestionado con implementación de Firewall. Se realiza anualmente, aunque.
EDM03-02. La empresa gestiona el riesgo crítico empresarial relacionado con las TI eficaz y eficientemente.	• Porcentaje de proyectos de la empresa que consideran el riesgo TI. • Porcentaje de planes de acción de riesgo TI ejecutados en tiempo. • Porcentaje de riesgos críticos que han sido eficazmente mitigados	30% 30% 15%	Los riesgos de TI casi no son tomados en cuenta en los proyectos de la institución. Se ha implementado a tiempo herramientas para disminuir los riesgos. Se ha implementado las medidas necesarias para su mitigación.
EDM03-03. Los riesgos empresariales relacionados con las TI no exceden el apetito de riesgo y el impacto del riesgo TI en el valor de la empresa es identificado y gestionado	• Nivel de impacto empresarial inesperado. • Porcentaje de riesgos TI que exceden el riesgo empresarial tolerado	80% 15%	El no contar con un apetito de riesgo actualizado aumenta la probabilidad de materialización de riesgos. No se conoce el% de riesgos actual en la Institución.

Cuadro 7
Autoevaluación EDM04. Asegurar la Optimización de Recursos

EDM04			
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.			
Meta del Proceso	**Metas Relacionadas**	**Cumple**	**Comentarios**
EDM04-01. Las necesidades de recursos de la empresa son cubiertas con capacidades óptimas.	• Nivel de realimentación de las partes interesadas sobre la optimización de los recursos	30%	Se realiza parcialmente la optimización de recursos.
	• Serie de beneficios (p.ej., ahorro de costes) que se logran a través de la utilización óptima de los recursos	20%	En base a la optimización de recursos se obtiene ahorro de costes.
	• Número de desviaciones del plan de recursos y las estrategias de arquitectura empresarial	0%	
EDM04-02. Los recursos se asignan para satisfacer mejor las prioridades de la empresa dentro del presupuesto y restricciones.	• Número de desviaciones (y excepciones) de los principios de Gestión de recursos	20%	No se dispone ciertos principios de Gestión de recursos.
	• Porcentaje de proyectos con asignación de recursos adecuados	10%	Los proyectos no disponen de recursos necesarios.
EDM04-03. El uso óptimo de los recursos se logra a lo largo de su completo ciclo de vida económico.	• Porcentaje de reutilización de componentes de la arquitectura	40%	Reutilizan los recursos disponibles.
	• Porcentaje de proyectos y programas con un estado de riesgo medio o alto debido a los problemas en la Gestión de recursos	20%	Se tiene un plan de Gestión de riesgos que no está vigente.
	• Número de metas de rendimiento de la Gestión de recursos alcanzadas	30%	No se tiene documentado las metas que han alcanzadas.

A continuación, se detalla el Resultado Final de la Evaluación Técnica Informática, realizada a los procesos de Gobierno de TI. El porcentaje obtenido está de acuerdo a la evaluación de cada uno de los procesos según los criterios y metas proporcionadas por COBIT 5, basándose en la evidencia documentada que fue recibida (ver cuadro 8).

Cuadro 8
Evaluación del nivel de cumplimiento los procesos EDM

DOMINIO EDM	PROCESOS	NIVEL DE CUMPLIMIENTO (%)				
		(0-20)	(20-40)	(40-60)	(60-80)	(80-100)
EDM01.	**EDM01.01**. Evaluar el Sistema de Gobierno		X			
	EDM01.02. Orientar el Sistema de Gobierno			X		
	EDM01.03. Supervisar el Sistema de Gobierno		X			
EDM02.	**EDM02.01**. Evaluar la Optimización del Valor			X		
	EDM02.02. Orientar la Optimización del Valor			X		
	EDM02.03. Supervisar la Optimización de Valor				X	
EDM03.	**EDM03.01**. Evaluar la Gestión de Riesgos			X		
	EDM03.02. Orientar la Gestión de Riesgos			X		
	EDM03.03. Supervisar la Gestión de Riesgos			X		
EDM04.	**EDM04.01**. Evaluar la Gestión de Recursos		X			
	EDM04.02. Orientar la Gestión de Recursos		X			
	EDM04.03. Supervisar la Gestión de Recursos		X			

De acuerdo al porcentaje del nivel de cumplimiento de los procesos de Gobierno de TI y luego de realizar un proceso de evaluación en base a evidencia analizada. Se ha corroborado que la UTIC, actualmente se encuentra elaborando un documento donde se encuentra incorporando normas, políticas y procedimientos que garanticen la continuidad del negocio, conjuntamente con los ejecutivos de la Institución.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Con la información proporcionada por la UTIC, se concluye que existe un compromiso en la mejora de sus procesos, es así que actualmente se cuenta una nueva estructura Orgánico-Funcional preliminar de la UTIC, que se encuentra enfocado a los proceso de Gobierno TI.

- Para garantizar los criterios emitidos en la Evaluación, fue necesario que los consultores se capaciten en el marco de referencia COBIT 5, proceso del cual se obtuvo la certificación en COBIT 5 IT Foundation.

- Con la realización de la Evaluación Técnica Informática, se determinó que la implementación de la norma 410, permite garantizar el correcto funcionamiento, la calidad de resultados y la mejora continua de las operaciones, así como también para detectar debilidades y riesgos potenciales de cada proceso que manejan Sistemas de Información.

- El personal que administra los Sistema de información, no ha recibido por parte de Talento Humano, las responsabilidades y funciones que tienen que desempeñar de acuerdo a su contratación específica, sin embargo, éstas han sido dadas a conocer por parte del Superior inmediato.

- Para lograr los propósitos establecidos dentro de una Evaluación Técnica es indispensable contar con toda la documentación que requiera el Consultor, esto permitirá evidenciar, cuál es la Situación Actual de una Empresa, hacia donde desea llegar y qué correcciones deben ser ejecutadas.

5.2 Recomendaciones

- Para que sea efectiva esta propuesta se necesita el apoyo oportuno de las máximas autoridades de la ESPE y se logre llevar a cabo la ejecución de los diferentes proyectos a realizarse en bien de la Comunidad Universitaria.

- Al realizar una Evaluación Técnica, se debe contar con el personal capacitado e idóneo, con experiencia en el manejo de los diferentes Marcos de Referencia, con el fin de garantizar los resultados emitidos.

- Se debería llevar un registro y control de cumplimiento de la Norma de Control Interno de la Contraloría General del Estado 410 en el área de la UTIC y monitorear el cumplimiento, de igual forma se debe socializar un grado de cultura de riesgos informáticos a todos los usuarios de la Institución.

- La Unidad de Talento Humano, debe entregar de manera formal las funciones, roles o responsabilidades al personal que administra los Sistemas de Información.

- El personal involucrado en una Evaluación Técnica debería prestar todas las facilidades al Consultor, con el fin determinar las falencias que deben ser corregidas a lo largo del proceso de la Evaluación Técnica.

BIBLIOGRAFÍA

Contraloría General del Estado. (01 de 12 de 2009). *Normatividad Vigente.* Obtenido de Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos: http://www.contraloria.gob.ec/documentos/normatividad/ACUERDO 039 CG 2009 5 Normas de Control Interno.pdf

Erb, M. (2012). *Gestión del Riesgo en la Seguridad Informática*. Obtenido de Análisi de Riesgo: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

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

ISACA. (2012). *COBIT 5*. Obtenido de Enabling Processes: www.isaca.org/COBITuse

ISACA. (2012). *Cobit 5 Procesos Catalizadores.* Madrid-España: ISACA.

ISACA. (2012). *Cobit 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Estados Unidos: ISACA.

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

Osiatis. (2012). *Ciclo de Vida de ITIL*. Obtenido de Osiatis: http://itilv3.osiatis.es/ciclo_vida_servicios_TI.php

GLOSARIO DE TÉRMINOS

UTIC: Unidad de Tecnologías de Información y Comunicaciones.

CMI: Cuadro de Mando Integral es un método para medir las actividades de una compañía en términos de su visión y estrategia.

PAM: Modelo de Evaluación de Procesos.

PRM: Modelo de Referencia de Procesos

PBRM: (plan, build, run and monitor) Planificar, Construir, Operar y Monitorear

NORMA 410: Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas emitidas por la Contraloría General del Estado en el 2009

ISACA: Asociación internacional encargada de apoyar y patrocinar el desarrollo de metodologías, métodos y certificaciones con respecto a la auditoría, seguridad y control de los sistemas de información.

COBIT: Control Objetives for Information and relatedTechnology (Objetivos de Control para tecnología de información y relacionada), metodología que propone un adecuado control de los proyectos de tecnología, flujos de información y los riesgos que la implementación de estas implica.

EFECTIVIDAD: Logro de los objetivos al menor costo y con el menor número de consecuencias imprevistas.