ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRIA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS

VI PROMOCIÓN

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE MAGISTER

TEMA:
"EVALUACIÓN TÉCNICA INFORMÁTICA DE LA ADQUISICIÓN E IMPLEMENTACIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE PRINCIPAL"

AUTORES: ING. ROSA ELVIRA PRUNA MADRIL

ING. JOHNNY CAMILO PRUNA MADRIL

DIRECTOR: ING. RUBÉN ARROYO MSc.

OPONENTE: ING. DARíO URVINA MSc.

SANGOLQUI

2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

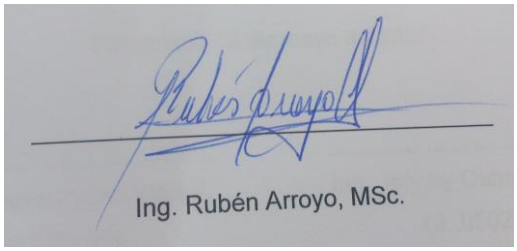
UNIDAD DE GESTIÓN DE POSGRADOS DECLARACIÓN DE RESPONSABILIDAD

TERMINACIÓN DE TESIS

Ing. Rubén Arroyo, MSc. CERTIFICA:

Que el trabajo titulado "**EVALUACIÓN TÉCNICA INFORMÁTICA DE LA ADQUISICIÓN E IMPLEMENTACIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE PRINCIPAL**." realizado por los señores ingenieros Rosa Elvira Pruna Madril con cédula de identidad número 0502631054 y Johnny Camilo Pruna Madril con cédula de identidad número 0502353519, está terminado, ha sido guiado y revisado periódicamente y cumple con las normas estatutarias establecidas.

Sangolquí, 13 de mayo de 2015



UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

UNIDAD DE GESTIÓN DE POSGRADOS DECLARACIÓN DE RESPONSABILIDAD

Nosotros, Rosa Elvira Pruna Madril y Johnny Camilo Pruna Madril

DECLARAMOS QUE:

El proyecto de posgrado denominado "**EVALUACIÓN TÉCNICA INFORMÁTICA DE LA ADQUISICIÓN E IMPLEMENTACIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE PRINCIPAL**" ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las referencias bibliográficas que constan en las páginas correspondientes y cuyas fuentes se incorporan en la bibliografía.

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, 12 de mayo de 2015

_____

Ing. Rosa Elvira Pruna Madril

CI. 0502631054

_____

Ing. Johnny Camilo Pruna Madril

CI. 0502353519

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

UNIDAD DE GESTIÓN DE POSGRADOS DECLARACIÓN DE RESPONSABILIDAD

AUTORIZACIÓN

Nosotros, Rosa Elvira Pruna Madril y Johnny Camilo Pruna Madril

Autorizamos a la Universidad de las Fuerzas Armadas la publicación, en la biblioteca virtual de la Institución del trabajo "**EVALUACIÓN TÉCNICA INFORMÁTICA DE LA ADQUISICIÓN E IMPLEMENTACIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE PRINCIPAL**.", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, 12 de mayo de 2015

_____

Ing. Rosa Elvira Pruna Madril
CI. 0502631054

_____

Ing. Johnny Camilo Pruna Madril
CI. 0502353519

AGRADECIMIENTO

Agradecemos al señor Ing. Rubén Arroyo, MSc., quién con su conocimiento, experiencia y apoyo ha permitido la consecución de este objetivo en nuestra carrera, muchas gracias por su impulso, consejo y ayuda durante el desarrollo del proyecto y sus magníficas enseñanzas como docente.

Agradecemos al señor Ing. Urvina López Darío Genaro, MSc, quién ha revisado de manera exhaustiva este trabajo de posgrado con la finalidad de que el mismo quede listo y completamente refinado.

Agradecemos al señor Ing. Mario Ron, MSc., coordinador del Proyecto de Auditoria aplicado a la ESPE, por el apoyo brindado en el tiempo que duró la maestría, así como con la acertada coordinación en el proceso de desarrollo de esta tesis, nuestro más sincero agradecimiento por su predisposición para apoyar las ideas e inquietudes de los maestrantes.

Gracias a todos nuestros familiares, quienes de una u otra forma, nos ayudaron para poder culminar con este proyecto, su tiempo y apoyo han sido vitales para que nosotros logremos culminar y cristalizar una más de nuestras metas trazadas en el ámbito profesional.

DEDICATORIA

Yo, Rosa Elvira Pruna Madril, dedico el presente trabajo de tesis, a mis hijos, esposo, padres y hermanos, en especial a mi hijo, por el sacrificio de soportar mi ausencia por el tiempo entregado a mencionada maestría, lo cual ha sido en gran manera vital para poder finalizar el presente proyecto de posgrado.

Yo, Johnny Camilo Pruna Madril dedico el presente trabajo de tesis, a todos y cada uno de los miembros de mi familia, en especial a mis padres y hermanos, quienes en todo momento me han mostrado su apoyo incondicional y con su ejemplo supieron inspirar en mí, un espíritu de superación constante.

INDICE GENERAL

TERMINACIÓN DE TESIS ii

DECLARAMOS iii

AUTORIZACIÓN iv

AGRADECIMIENTO v

DEDICATORIA vi

INDICE..... vii-viii

INDICE TABLAS..... IX

INDICE FIGURAS..... X

CAPITULO I. INTRODUCCION 1

1.1 Antecedentes 1
1.2 Planteamiento del Problema 1
1.3 Formulación del Problema 2
1.4 Justificación del Problema 2
1.5 Objetivo General 3
1.6 Objetivos Específicos 3

CAPÍTULO II. FUNDAMENTACION TEORICA 4

2.1 Antecedentes..... 4
2.2 Cobit 5..... 4
2.2.1 Los cinco principios de COBIT 5..... 4
2.2.1.1 Principio 1. Satisfacer las necesidades de los interesados..... 5
2.2.1.2 Principio 2. Cubrir la empresa de extremo a extremo..... 5
2.2.1.3 Principio 3. Aplicar un solo marco integrado..... 5
2.2.1.4 Principio 4. Habilitar un enfoque Holístico..... 5
2.2.1.5 Principio 5.Separar el gobierno de Administración..... 6
2.2.2 Dominios de COBIT 5..... 7
2.2.1.1 Evaluar, Orientar y Supervisar (EDM)..... 7
2.2.2.2 Alinear, Planificar y Organizar (APO) 7
2.2.2.3 Construir, Adquirir e Implementar (BAI) 7
2.2.2.4 Entrega, Servicio y Soporte (DSS) 7
2.2.2.5 Supervisar, Evaluar y Valorar (MEA)
2.3 Administración de Riesgos 5..... 8
2.3.1 Control de riesgos..... 8
2.3.2 Riesgos..... 9
2.3.3 Técnicas de Procedimientos para Administrar Riesgos..... 9

2.3.4 Medición y Evaluación del Riesgo……..……...9
2.3.5 Sistemas de Control de Riesgos……...10
2.3.6 Programa de Trabajo……..……11
2.4 Auditoría Informática……..……..…11
2.4.1 Perfiles Profesionales de la Función de Auditoría …..……..…11
2.4.2 Objetivos de la Auditoría Informática……12
2.4.3 Bases De La Auditoría Informática ……12
2.4.4 Funciones De La Auditoría Informática……...12
2.4.5 Metodología de Desarrollo de la Auditoría Informática……13
2.5 Marco Conceptual……...13
2.5.1 COBIT 5……..13
2.5.2 Dominio Construir, Adquirir e Implementar……13
2.6 Estado Del Arte……..16
2.6.1 Fases de la Auditoria ……16
CAPÍTULO III. METODOLOGIA DE INVESTIGACION 19
3.1 Descripción de la Metodología 19
3.1.1 Método de Trabajo y Procedimientos a Ejecutar 20
3.1.2 Productos a Entregar..... 20
3.1.3 Herramientas a Utilizar 20
3.2 Caracterización preliminar..... 21
3.3 Matriz de Riesgos
……..213
3.4 Plan de Investigación de Campo……25
3.5 Elaboración de Instrumentos de investigación de campo..... 49
3.6 Aplicación de Instrumentos de investigación de campo 4950
3.7 Análisis de la información..... 50
CAPITULO IV. INFORME FINAL 51
4.1 Informe Ejecutivo..... 51
4.1.1 Antecedentes 51
4.1.2 Descripción Metodológica 51
4.1.3 Principales hallazgos.....52
4.1.4 Conclusión 544
4.1.5 Recomendación.....55
4.2 Informe Detallado.....55
4.3 Evidencias. 800
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 811
5. 1 Conclusiones y Recomendaciones 811
5.2 Conclusiones 811
5.3 Recomendaciones.....822
BIBLIOGRAFÍA 84
ANEXOS.....87

INDICE DE TABLAS

Tabla 1: Tipos de Riegos……..…….9
Tabla 2: Técnicas de Procedimientos Administración Riesgos…..……9
Tabla 3: Sistemas de Control de Riesgos……10
Tabla 4: Programa de Trabajo Control de Riesgos…….……10
Tabla 5: Perfil Profesional – Auditoría Informática……..11
Tabla 6: Objetivos de Auditoría Informática……..……11
Tabla 7: Funciones de Auditoría Informática……..12
Tabla 8: Metodología de Auditoría Informática……12
Tabla 9: Controles del Dominio Adquirir e Implementar……..……..13
Tabla 10: Fases de Auditoría Informática…….……16
Tabla 11: Matriz de Riesgos …….…….22
Tabla 12: Plan de Investigación de Campo…….…….26

INDICE DE FIGURAS

Figura1: Principios de COBIT 5 ……..4
Figura2: Principio 1. Satisfacer las necesidades de los interesados……..5
Figura3: Habilitadores de COBIT5 …...…….6
Figura 4: Gobierno y Administración……..…….6
Figura 5: Cadena de Valor…….……8
Figura 6: Bases de la Auditoria Informática……..……12

CAPITULO I. INTRODUCCION

1.1 Antecedentes

Desde hace algunos años, la Universidad de las Fuerzas Armadas ESPE, ha venido ejecutando varios proyectos en el área informática, con el objeto de apoyar a las diferentes actividades que desarrolla la Universidad.

Se han implementado algunos servicios informáticos y otros se encuentran en desarrollo, para lo que se han adquirido equipos, instalado redes y contratado servicios adicionales.

La Universidad de las Fuerzas Armadas ESPE, como una Institución Educativa de Prestigio que brinda servicios académicos de alta calidad, cuenta con una Unidad de Tecnología de Información y Comunicación UTIC que centraliza la administración y gestión de las actividades de TI, es decir se encarga del análisis, desarrollo e implantación de los sistemas requeridos en la ESPE y se preocupa por el adecuado funcionamiento de las aplicaciones existentes, redes y comunicaciones.

Por lo expuesto se ha elaborado y aprobado formalmente el Proyecto para realizar la Evaluación Técnica Informática de la Universidad de las Fuerzas Armadas, con la finalidad de asegurar que los objetivos de Gobierno de TI, se hayan cumplido en la Institución. Para este proyecto se utilizará como marco de referencia COBIT estándar Internacional.

1.2 Planteamiento del Problema

Actualmente la Universidad de las Fuerzas Armadas ESPE sede principal, se encuentra en un proceso de cambio a nivel institucional, por tanto tiene problemas con la evaluación, orientación y supervisión en el área de Gobierno TI, debido principalmente al permanente cambio de autoridades y a la falta de herramientas apropiadas en esta área que ayuden a llevar una administración adecuada.

1.3 Formulación del Problema

¿Los nuevos proyectos que estén en camino ofrecen soluciones que satisfagan las necesidades de la Institución?

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

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

Para la Evaluación Técnica Informática de la Adquisición e Implementación se utilizará el marco de referencia internacional COBIT 5 específicamente para este caso el Dominio de Adquisición e Implementación; al finalizar la evaluación se emitirá recomendaciones a la Institución ESPE de los riesgos que tiene el Área Informática y los procedimientos adecuados para mitigarlos o eliminarlos.

1.4 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 obtener ventaja competitiva.

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 entre otros, para establecer el GAP, que será minimizado 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.

1.5 Objetivo General

Evaluar la Adquisición e Implementación de la Universidad de las Fuerzas Armadas ESPE Sede Principal, aplicando como marco de referencia COBIT 5, con el fin de crear valor para la Institución.

1.6 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 los Informes.
- Presentar los informes y acoger los puntos de vista.

CAPÍTULO II. FUNDAMENTACION TEORICA

2.1 Antecedentes

La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen funcionamiento de una organización y para el aseguramiento de su supervivencia en el mercado. COBIT 5 es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a los sectores de una organización, es decir, administradores IT, usuarios y los auditores involucrados.

2.2 COBIT 5

COBIT 5 ayuda a las Organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos. COBIT 5 permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios.

2.2.1 Los cinco principios de COBIT 5

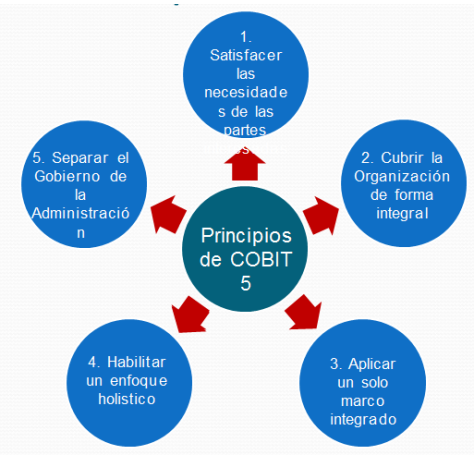


Figura1: Principios de COBIT 5

Fuente: http://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt

2.2.1.1 Principio 1. Satisfacer las necesidades de los interesados.

Las Empresas tienen **muchos** interesados, y **"crear valor"** significa diferentes y a veces contrarias cosas a cada uno. Gobernar es acerca de negociar y decidir entre los diferentes interesados.

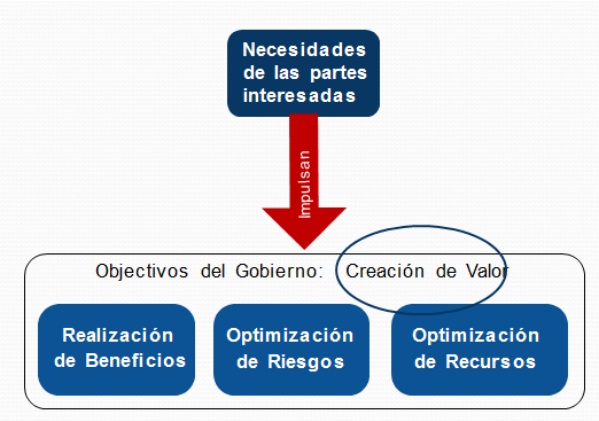


Figura2: Principio 1. Satisfacer las necesidades de los interesados

Fuente: http://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt

2.2.1.2 Principio 2. Cubrir la empresa de extremo a extremo.

Esto significa que COBIT 5, integra el gobierno empresarial de TI en el gobierno corporativo. Cubre todas las funciones y procesos dentro de la empresa. (COBIT® 5, ISACA)

2.2.1.3 Principio 3. Aplicar un solo marco integrado.

COBIT 5 se alinea con los estándares y marcos más relevantes usados por las empresas: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 38500, ITIL, serie ISO/IEC 27000, TOGAF, Etc. (COBIT® 5, ISACA)

2.2.1.4 Principio 4. Habilitar un enfoque Holístico.

Se describen los habilitadores de COBIT 5 en **siete categorías:**

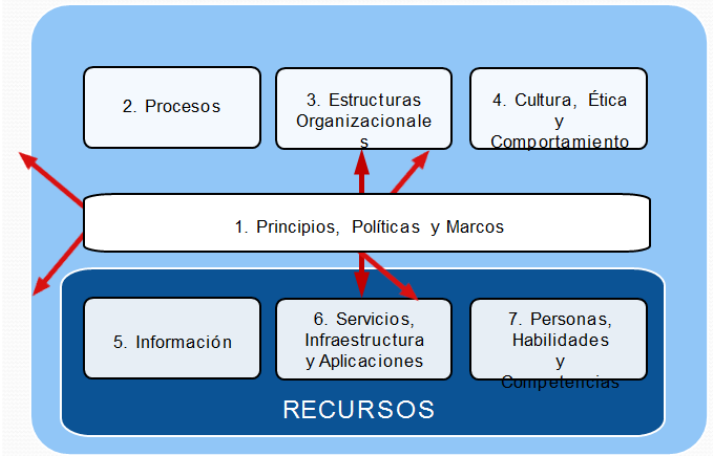


Figura3: Habilitadores de COBIT 5

Fuente: http://www.ccpa.or.cr/file/isaca/dia1/5-evolucion-de-cobit-4-1-a-5-alvaro-jaikel.pdf

2.2.1.5 Principio 5. Separar Gobierno de Administración.

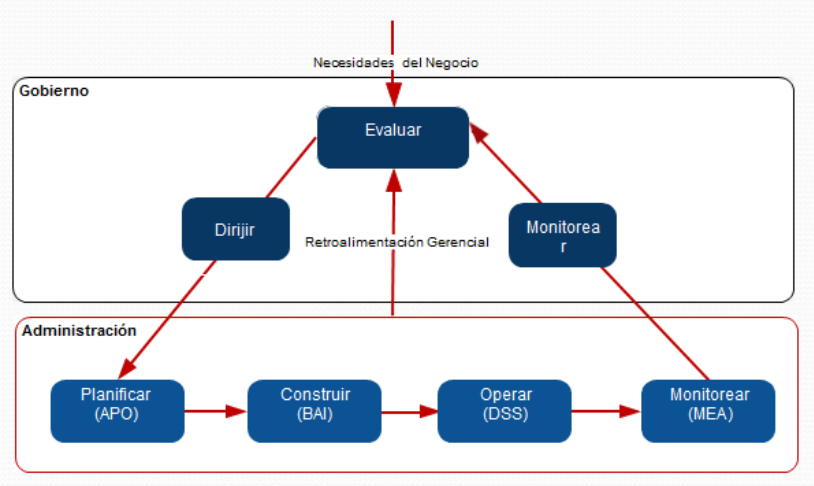


Figura 4: Gobierno y Administración

Fuente: http://www.ccpa.or.cr/file/isaca/dia1/5-evolucion-de-cobit-4-1-a-5-alvaro-jaikel.pdf

Gobierno - Responsabilidad de la Junta Directiva.

Administración - Responsabilidad de la alta administración.

2.2.2 Dominios de COBIT5.

2.2.2.1 Evaluar, Orientar y Supervisar (EDM)

Dominio de GOBIERNO, que contiene cinco procesos de gobierno, dentro de cada proceso, evaluar, dirigir y supervisar. (COBIT® 5, ISACA)

2.2.2.2 Alinear, Planificar y Organizar (APO)

Dominio de GESTIÓN, que cubre la gestión de TI con base a estrategia, tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. (COBIT® 5, ISACA)

2.2.2.3 Construir, Adquirir e Implementar (BAI)

Dominio de GESTIÓN, Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. (COBIT® 5, ISACA)

2.2.2.4 Entrega, Servicio y Soporte (DSS)

Dominio de GESTIÓN, que hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. (COBIT® 5, ISACA)

2.2.2.5 Supervisar, Evaluar y Valorar (MEA)

Dominio de GESTIÓN, que hace referencia a que todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control. Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos

de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. (COBIT® 5, ISACA)

2.3 Administración de Riesgos.

La Administración y análisis de Riesgos constituye una herramienta muy importante para el trabajo del auditor y la calidad del servicio, por cuanto implica el diagnóstico de los mismos para velar por su posible manifestación o no.

La administración de riesgos en un marco amplio implica que las estrategias, procesos, personas, tecnología y conocimiento están alineados para manejar toda la incertidumbre que una organización enfrenta. (BUITRAGO)

2.3.1 Control de Riesgos.

Técnica diseñada para minimizar los posibles costos causados por los riesgos a que esté expuesta la organización, esta técnica abarca el rechazo de cualquier exposición a pérdida de una actividad particular y la reducción del potencial de las posibles pérdidas. La Cadena de Valores en todos los subprocesos de Auditoría, debe representarse de la siguiente forma:

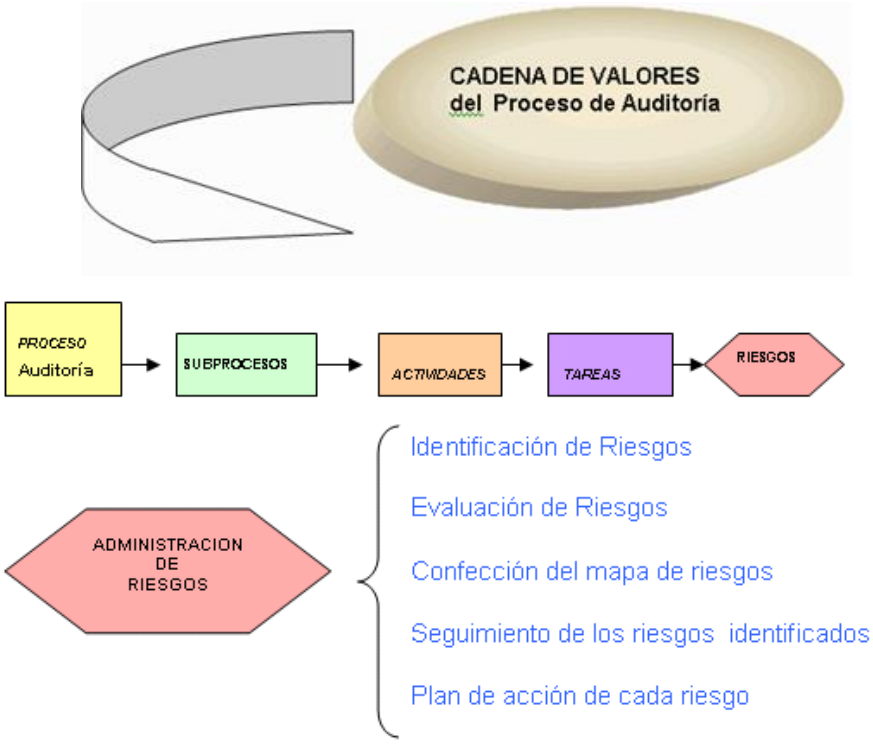


Figura 5: Cadena de Valor

Fuente: http://catarina.udlap.mx/u_dl_a/tales/documentos/lat/salgado_a_a/capitulo2.pdf

2.3.2 Riesgos.

El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de pérdidas. Generalmente se habla de Riesgo en la evolución de los Sistemas de Control Interno, donde se asume 3 tipos de Riesgo:

Tabla 1

Tipos de Riegos

RIESGO DE CONTROL	Se propicia por falta de control de las actividades y puede generar deficiencias del Sistema de Control.
RIESGO DE DETECCIÓN	Es aquel que en su revisión no detecten deficiencias en el Sistema de Control Interno.
RIESGO INHERENTE	Son aquellos que se presentan inherentes a las características del Sistema de Control Interno

Fuente: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

2.3.3 Técnicas de Procedimientos para Administrar Riesgos.

Tabla 2

Técnicas de Procedimientos Administración Riesgos

EVITAR RIESGOS	Un riesgo es evitado cuando en la organización no se acepta.
REDUCCIÓN DE RIESGOS	Los riegos pueden ser reducidos para evitar futuras pérdidas con la asesoría de personas expertas.
CONSERVACIÓN DE RIESGOS	Es quizás el más común de los métodos para enfrentar los riesgos.
COMPARTIR RIESGOS	Cuando los riesgos son compartidos, la posibilidad de pérdida es transferida del individuo al grupo.

Fuente:http://www.monografias.com/trabajos47/riesgos-auditoria-interna/riesgosuditoria-interna.shtm

2.3.4 Medición y Evaluación del Riesgo.

Al concebir los posibles Riesgos en la ejecución de los diferentes subprocesos de la Auditoría de una organización interna o externa, debe efectuarse la evaluación de los mismos, con el fin de conocer el Impacto, y el tratamiento que este requiere, así como la probabilidad de ocurrencia.

Lo que generaría la posibilidad de conocer anticipadamente la valoración y concepción de planes que coadyuven a la reducción de pérdidas, que en técnicas de auditoría, serían la extensión de pruebas innecesarias, y gasto de tiempo invertido adicional, lo que implicaría el requerimiento de tratamientos diferenciados, y por supuesto pérdidas financieras. (ECHEVERRY)

2.3.5 Sistemas de Control de Riesgos.

La estructura de Control de Riesgos pudiéramos fundamentarla en dos pilares:

Tabla 3

Sistemas de Control de Riesgos

SISTEMAS	CARACTERISTICAS	OBJETIVOS
SISTEMAS COMUNES DE GESTIÓN	Estos sistemas desarrollan las normas internas y su método para la evaluación y el control de los riesgos y representan una cultura común en la gestión de los negocios, compartiendo el conocimiento acumulado y fijando criterios	• Identificar posibles • Optimizar la gestión diaria • Fomentar la sinergia y creación de valor • Reforzar la identidad corporativa
AUDITORÍA INTERNA	Está estructurada alrededor de los Servicios Mancomunados de Auditoría, que engloban los equipos de auditoría de las Unidades de Negocio y Servicios Corporativos	• Prevenir los riesgos • Controlar la aplicación y promocionar el desarrollo • Crear valor y promover la construcción

Fuente: http://wwwdiariomedico.com/gestion/ges.220300.com

2.3.6 Programa de Trabajo.

Tabla 4

Programa de Trabajo Control de Riesgos

PROGRAMA	CARACTERISTICAS	OBJETIVOS
OBTENCIÓN Y EVALUACIÓN DE EVIDENCIA	El auditor deberá obtener evidencia suficiente y apropiada en la auditoría para poder extraer conclusiones.	• Evidenciar la auditoría • Pruebas de control. • Procedimientos sustantivos.
DOCUMENTACIÓN	El auditor deberá documentar los asuntos que son importantes para apoyar las conclusiones expresadas en el informe de auditoría y dejar evidencia de que la auditoría se llevó a cabo de acuerdo a normas y técnicas señaladas por los organismos profesionales.	• Apoyar en la planeación y ejecución • Apoyar en la supervisión y revisión • Registrar la evidencia de la auditoría resultante.

Fuente: http://wwwdiariomedico.com/gestion/ges.220300.com

2.4 Auditoría Informática

La auditoría informática, parte de los años cincuenta cuando las organizaciones empezaron a desarrollar aplicaciones informáticas. Donde la auditoría trataba con sistemas manuales. Posteriormente, en función de que las organizaciones empezaron con sistemas cada vez más complejos, se hizo necesario que parte del trabajo de auditoría empezara a tratar con sistemas que utilizaban sistemas informáticos. En ese momento, los equipos de auditoria, tanto externos como internos, empezaron a ser mixtos, con involucración de auditores informáticos junto con auditores financieros. (LEAL)

2.4.1 Perfiles Profesionales de la Función de Auditoría Informática.

En relación a lo que se mencionaba anteriormente, se ve claramente que el auditor informático debe ser una persona con un alto grado de calificación técnica y al mismo tiempo estar integrado en las corrientes organizativas empresariales que imperan hoya. Por tanto se debe contemplar las siguientes características para mantener un perfil profesional adecuado y actualizado:

Tabla 5

Perfil Profesional – Auditoría Informática

PERSONAS	Deben contemplar conocimientos básicos en : • Desarrollo, gestión, ciclo de vida de proyectos. • Gestión del departamento de sistemas. • Análisis de riesgos del entorno informático
SISTEMA OPERATIVO	• Depende de varios factores: • Entorno único - auditor interno • Varios entornos - auditor externo

Fuente:http://www.monografias.com/trabajos14/auditoriaistemas/auditoriasistemas.shtml

2.4.2 Objetivos de la Auditoría Informática.

Tabla 6

Objetivos de Auditoría Informática

OBJETIVOS	Protección de activos e integridad de datos
	Gestión de protección de activos
	Gestión de protección eficiente y eficaz

Fuente: (Piattini, 2011)

2.4.3 Bases De La Auditoría Informática.

Figura 6: Bases de la Auditoria Informática

Fuente: (Serafín Simón, 2006)

2.4.4 Funciones De La Auditoría Informática.

Los elementos indispensables para cumplir este requisito son:

Tabla 7

Funciones de Auditoría Informática

FUNCIONES	**PLANEACIÓN CONTROL**	• Los recursos informáticos deben ser orientados al logro de los objetivos y estrategias. • Elaboración, difusión y cumplimiento de políticas, controles y procedimientos. • Resultados esperados en base a la coordinación.
	SEGUIMIENTO	

Fuente: (Piattini, 2011)

2.4.5 Metodología de Desarrollo de la Auditoría Informática.

Se contemplan las siguientes fases:

Tabla 8

Metodología de Auditoría Informática

FASE 1	Identificar el alcance y los objetivos de la Auditoría Informática
FASE 2	Realizar el estudio inicial del entorno a auditar
FASE 3	Determinación de los recursos necesarios para realizar la auditoría informática
FASE 4	Elaborar el plan de trabajo
FASE 5	Realizar las actividades de auditoría
FASE 6	Realizar el informe final
FASE 7	Carta de Presentación

Fuente: Kuna (2012)

2.5 Marco Conceptual

2.5.1 COBIT 5

2.5.2 Dominio Construir, Adquirir e Implementar

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos de la Institución. Además el cambio y mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos de la Institución.

Tabla 9

Controles del Dominio Adquirir e Implementar

CONTROLES	OBJETIVOS
BAI1. IDENTIFICAR SOLUCIONES AUTOMATIZADAS	BAI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio. BAI1.2 Reporte de análisis de riesgos BAI1.3 Estudio de factibilidad y formulación de cursos de acción alternativos BAI1.4 Requerimientos, decisión de factibilidad y aprobación
BAI2.ADQUIRIR Y MANTENER SOFTWARE APLICATIVO	BAI2.1 Diseño de alto nivel BAI2.2 Diseño detallado BAI2.3 Control y audibilidad de las aplicaciones BAI2.4 Seguridad y disponibilidad de las aplicaciones BAI2.5 Configuración e implantación de software aplicativo adquirido BAI2.6 Actualizaciones importantes en sistemas existentes BAI2.7 Desarrollo de software aplicativo: BAI2.8 Aseguramiento de la Calidad del Software BAI2.9 Administración de los requerimientos de aplicaciones BAI2.10 Mantenimiento de software aplicativo
BAI3. ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA	BAI3.1 Plan de adquisición de infraestructura tecnológica BAI3.2 Protección y disponibilidad del recurso de infraestructura BAI3.3 Mantenimiento de la Infraestructura BAI3.4 Ambiente de prueba de factibilidad
BAI4. FACILITAR LA OPERACIÓN Y EL USO	BAI4.1 Plan para soluciones de operación BAI4.2 Transferencia de conocimiento a la gerencia del negocio BAI4.3 Transferencia de conocimiento a usuarios finales BAI4.4 Transferencia de conocimiento al personal de operaciones y soporte
BAI5. ADQUIRIR RECURSOS DE TI	BAI5.1 Control de adquisición BAI5.2 Administración de contratos con proveedores: BAI5.3 Selección de proveedores: BAI5.4 Adquisición de las TI:
BAI6. ADMINISTRAR CAMBIOS	BAI6.1 Estándares Procedimientos para Cambios BAI6.2 Evaluación de Impacto, Priorización y Autorización

CONTINÚA

	BAI6.3 Cambios de Emergencia BAI6.4 Seguimiento y Reporte del Estatus de Cambio BAI6.5 Cierre y Documentación de Cambio
BAI7. INSTALAR Y ACREDITAR SOLUCIONES Y CAMBIOS	BAI7.1 Entrenamiento BAI7.2 Plan de Prueba BAI7.3 Plan Implementación BAI7.4 Ambiente de Prueba BAI7.5 Conversión Sistema y Datos BAI7.6 Prueba de Cambios BAI7.7 Prueba de Aceptación Final BAI7.8 Promoción a Producción BAI7.9 Revisión Posterior a la Implantación
BAI08. GESTIONAR EL CONOCIMIENTO	BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos. BAI08.02 Identificar y clasificar las fuentes de información. BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento. BAI08.04 Utilizar y compartir el conocimiento. BAI08.05 Evaluar y retirar la información.
BAI09. GESTIONAR LOS ACTIVOS	BAI09.01 Identificar y registrar los activos actuales. BAI09.02 Gestionar Activos Críticos. BAI09.03 Gestionar el ciclo de vida de los activos. BAI09.04 Optimizar el coste de los activos. BAI09.05 Administrar Licencias
BAI10.GESTIONAR LA CONFIGURACIÓN	BAI10.01 Establecer y mantener un modelo de configuración. BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia. BAI10.04 Generar informes de estado y configuración. BAI10.05 Verificar y revisar la integridad del repositorio de configuración.

Fuente: http://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt

2.6 Estado Del Arte

2.6.1 Fases de la Auditoria

Tabla 10

Fases de Auditoría Informática

FASES	CARACTERISTICA	
PLANEACIÓN	La planeación deberá ser documentada e incluirá:	• La planeación de la auditoría • El examen y la evaluación • La comunicación de resultados
REVISIÓN PRELIMINAR	Consiste obtener la información necesaria para que el auditor pueda tomar la decisión de cómo proceder en la auditoría.	• Diseño de la auditoría. • Revisión detallada de los controles internos. • No confiar en los controles
REVISIÓN DETALLADA	En la fase de evaluación detallada es importante para el auditor identificar las causas de las pérdidas existentes dentro de la instalación y los controles para reducir las pérdidas y los efectos causados por éstas.	• Los objetivos de la fase detallada son los de obtener la información necesaria para que el auditor tenga un profundo entendimiento de los controles usados dentro del área de informática.
EXAMEN Y EVALUACIÓN DE LA INFORMACIÓN	Los auditores deberán obtener, analizar, interpretar y documentar la información para apoyar los resultados de la auditoría. El proceso de examen y evaluación de la información es el siguiente:	• Obtener la información de los objetivos y alcances. • Supervisar para proporcionar seguridad. • Revisión por la gerencia de auditoría. • Reportar los resultados • Discutir las conclusiones y recomendaciones en los niveles apropiados de la administración antes de emitir su informe final.
PRUEBAS DE CONTROLES DE USUARIO	Las pruebas que compensan las deficiencias de los controles internos se pueden realizar mediante cuestionarios, entrevistas, visitas y evaluaciones hechas directamente con los usuarios.	
PRUEBAS SUSTANTIVAS	El objetivo es obtener evidencia suficiente que permita al auditor emitir su juicio en las conclusiones. El auditor externo expresará este juicio en forma de opinión sobre cuándo puede existir un proceso equivocado o falta de control. Se pueden identificar ocho diferentes pruebas sustantivas:	Pruebas: • Para asegurar la calidad • Para identificar la inconsistencia • Para comparar con los datos o contadores físicos. • Confirmación de datos con fuentes externas. • Para confirmar la adecuada comunicación. • Para determinar falta de seguridad.

CONTINÚA

		• Para determinar problemas de legalidad
EVALUACIÓN DE LOS SISTEMAS DE ACUERDO AL RIESGO	Son aquellos objetos, dispositivos, medidas, etc. que contribuyen a hacer más seguro el funcionamiento o el uso.	
INVESTIGACIÓN PRELIMINAR	Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos: Administración y Sistemas	**Administración** • Objetivos a corto y largo plazo. • Recursos materiales y técnicos • Solicitar documentos sobre los equipos, número de ellos, localización y características. • Fechas de instalación de los equipos y planes de instalación. • Contratos vigentes de compra, renta y servicio de mantenimiento. • Contratos de seguros. • Configuración de los equipos y capacidades actuales y máximas. • Planes de expansión. • Políticas de operación y uso **Sistemas** • Descripción general de los sistemas instalados y de los que estén por instalarse. • Manual de formas y procedimientos. • Descripción genérica. • Diagramas de entrada, archivos, salida. • Fecha de instalación. • Proyecto de instalación de nuevos sistemas.
PERSONAL PARTICIPANTE	Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervenga esté debidamente capacitado, que tenga un alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo. Con estas bases debemos considerar los conocimientos, la práctica profesional y la capacitación que debe tener el personal que intervendrá en la auditoria.	
RECOPILACIÓN DE LA INFORMACIÓN ORGANIZACIONAL	Una vez elaborada la planeación de la auditoría, la cual servirá como plan maestro de los tiempos, costos y prioridades, y como medio de control de la auditoría, se debe empezar la recolección de la información.	

CONTINÚA →

ENTREVISTA CON EL PERSONAL DE INFORMÁTICA	Puede entrevistarse a un grupo de personas elegidas, sus opiniones deben ser debidamente fundamentadas.	Las opiniones determinan: • Grado de cumplimiento de la estructura organizacional. • Grado de cumplimiento de las políticas y los procesos. • Satisfacción e insatisfacción • Capacitación y observaciones generales
INFORME DE LA AUDITORIA INFORMÁTICA	El informe es el documento escrito mediante el cual la comisión de auditoría expone el resultado final de su trabajo, a través de juicios fundamentados en las evidencias obtenidas durante la fase de ejecución, con la finalidad de brindar suficiente información a los funcionarios de la entidad auditada, sobre las deficiencias o desviaciones más significativas, e incluir las recomendaciones que permitan mejoras en la conducción de las actividades u operaciones de las áreas examinadas.	• Estructura: • Introducción • Origen del Examen • Naturaleza y Objetivos del Examen • Alcance del examen • Antecedentes y base legal de la entidad • Comunicación de hallazgos • Observaciones • Conclusiones • Recomendaciones • Anexos • Firma

Fuente:http://www.monografias.com/trabajos47/riesgos-auditoria-interna/riesgos-auditoria-interna.shtml

CAPÍTULO III. METODOLOGIA DE INVESTIGACION

3.1 Descripción de la Metodología

La metodología a utilizarse en el proyecto de tesis es COBIT 5 marco de referencia integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 proporciona la guía de nueva generación de ISACA para el gobierno y la gestión de las TI en las empresas. Se construye sobre más de 15 años de uso práctico y aplicación de COBIT por parte de muchas empresas y usuarios de las comunidades de negocio, TI, riesgo, seguridad y aseguramiento.

Modelo de referencia que tiene la facilidad de adaptarse a cualquier tipo de negocio y a los objetivos de control que se han definido en el modelo, pueden ser aplicados independientemente del ambiente, plataformas y madurez tecnológica de la organización; por lo que se proyecta aplicar el Marco Referencial COBIT 5, adaptado a la Universidad de las Fuerzas Armadas ESPE Sede Principal, que se sujeta a prácticas de administración a través de objetivos de control de alto nivel, organizadas en 1 dominio de gobernabilidad y cuatro dominios de gestión; estructura basada en 5 principios y 7 catalizadores. 37 procesos en total, 5 para gobierno y 32 para gestión.

- Evaluar, Orientar y Supervisar (Dominio Gobierno)
- Alinear, Planificar y Organizar (Dominio Gestión)
- Construir, Adquirir e Implementar (Dominio Gestión)
- Entregar, dar servicio y Soporte (Dominio Gestión)
- Supervisar, Evaluar y Valorar (Dominio Gestión)

Dominios que sujetan declaraciones de los resultados que se desean obtener, mediante la implementación de procedimientos de controles específicos y relacionados a la actividad TI, en función de los riesgos identificados y focalizados en el Departamento de la UTIC de la Universidad de las Fuerzas Armadas ESPE Sede Principal.

3.1.1 Método de Trabajo y Procedimientos a Ejecutar

Durante la auditoría, se debe recopilar información útil y necesaria, la cual debe ser analizada para obtener conclusiones, que luego derivan en recomendaciones para el mejoramiento de la organización. La obtención de información o evidencias, se puede realizar combinando uno o más de los siguientes procedimientos:

- Preguntar y confirmar
- Recolectar y analizar evidencia
- Inspeccionar
- Recalcular y analizar

3.1.2 Productos a Entregar

En base a la revisión y análisis llevada a cabo, se identificarán las debilidades de control en el Departamento de la UTIC. Se elaborará un informe ejecutivo y un informe detallado el cual será presentado al finalizar el proyecto.

Las recomendaciones emitidas en base a las debilidades identificadas dependiendo de la factibilidad y posibilidad de la empresa, deberán ser implementadas a futuro para luego ser evaluado en un nuevo proyecto.

3.1.3 Herramientas a Utilizar

La auditoría informática, se basa en una serie de análisis que se realiza con un método base seleccionado para la realización de este trabajo:

- Encuestas (Cuestionario) de evaluación acerca de los programas o proyectos

Además existen otros métodos, como son:

- Matrices de Investigación de Campo

Instrumento elaborado para ser utilizado como base de datos para la organización del trabajo del Equipo de Auditores.

- Observación Directa

Técnica que nos permite captar con todos nuestro sentido la realidad de la organización y puede ser de dos tipos. No participante, es decir aquella en que el auditor o grupo de auditores no interfiere en el proceso de auditoría y participante, es aquella en la que el auditor o grupo de auditores participa en los procesos de la unidad auditada, integrándose en el grupo y sus actividades. En cualquiera de los casos, hay que definir el objetivo, las variables, la planificación y trascripción de la observación.

3.2 Caracterización preliminar

Como primera actividad se espera Recolectar y analizar evidencia, para luego confirmar y determinar si los programas o proyectos mantienen la integridad de los datos y, principalmente si lleva a cabo eficazmente los fines de la organización, utilizando eficientemente los recursos.

Este trabajo se ejecutará en el Departamento de la UTIC de la Universidad de las Fuerzas Armadas ESPE Sede Principal, para lo cual se realizará la revisión de documentación de programas y proyectos del año 2014 establecidos dentro de la institución, aplicando el modelo COBIT 5.

Proyecto de tesis que tendrá una duración de 20 semanas, al finalizar la auditoría se espera obtener recomendaciones en base a las falencias detectadas, hallazgos que nos permitirán generar recomendaciones que quedarán trazadas o planteadas en el informe final, para que luego puedan ser aplicadas según criterio de las autoridades.

3.3 Matriz de Riesgos

La Matriz en mención resume procesos y prácticas de gestión más críticos del dominio Construir, adquirir e implementar en base al modelo de referencia COBIT 5, Metodología a utilizar para la ejecución del proyecto de tesis. Previo a un análisis se identificó en la matriz de riesgos los **PROCESOS y PRACTICAS DE GESTIÓN** más relevantes **de la adquisición e implementación de la UTIC ESPE (Sede principal)**.

Tabla 11
Matriz de Riesgos

MATRIZ DE RIESGOS CRÍTICOS DE LA ADQUISICIÓN E IMPLEMENTACIÓN DE LA ESPE (SEDE PRINCIPAL)										
PROCESOS Y PRACTICAS DE GESTIÓN	**Nivel de Riesgo**			**Nivel de Impacto**			**Auditable**		**Documentación Actualizada**	
	Alto	Medio	Bajo	Alto	Medio	Bajo	SI	NO	SI	NO
Construir, Adquirir e Implementar (BAI)										
BAI01 Gestionar los programas y Proyectos										
BAI01.01 Mantener un enfoque estándar para la gestión de programas y proyectos.	X			X			X			X
BAI01.02 Iniciar un programa.	X			X			X			X
BAI01.03 Gestionar el compromiso de las partes interesadas.	X			X			X			X
BAI01.04 Desarrollar y mantener el plan de programa.	X			X			X			X
BAI01.05 Lanzar y ejecutar el programa.	X			X			X			X
BAI01.06 Supervisar, controlar e informar de los resultados del programa	X			X			X			X
BAI01.07Lanzar e iniciar proyectos dentro de un programa.		X			X		X			X
BAI01.08 Planificar proyectos.		X			X		X			X
BAI01.09Gestionar la calidad de los programas y proyectos.	X			X			X			X
BAI01.10 Gestionar el riesgo de los programas y proyectos.	X			X			X			X
BAI01.11 Supervisar y controlar proyectos.	X			X			X			X

CONTINÚA

BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto.	X		X		X		X	
BAI01.13 Cerrar un proyecto o iteración.	X		X		X		X	
BAI01.14 Cerrar un programa.	X		X		X		X	
BAI02 Gestionar la definición de requisites								
BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio.	X		X		X		X	
BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas.	X		X		X		X	
BAI02.03 Gestionar los riesgos de los requerimientos.	X		X		X		X	
BAI02.04 Obtener la aprobación de los requerimientos y soluciones	X		X		X		X	
BAI04 Gestionar la Disponibilidad y la Capacidad								
BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.	X		X		X		X	
BAI04.02 Evaluar el impacto en el negocio.	X		X		X		X	
BAI04.03 Planificar requisitos de servicio nuevos o modificados.		X		X	X		X	
BAI04.04 Supervisar y revisar la disponibilidad y la capacidad.	X		X		X		X	
BAI06 Gestionar los Cambios								
BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio.	X		X		X		X	
BAI06.02 Gestionar cambios de emergencia.	X		X		X		X	
BAI06.03 Hacer seguimiento e informar de cambios de estado.	X		X		X		X	
BAI06.04 Cerrar y documentar los cambios.	X		X		X		X	

Fuente: UTIC – ESPE

En base a la matriz de riesgos, se estructura el plan de investigación de campo.

3.4 Plan de Investigación de Campo.

Los datos para el diagnóstico son tomados en base a modelo de referencia COBIT 5, se diseñó una tabla en Excel considerando el dominio objeto de estudio, que contempla los procesos, prácticas de gestión y actividades. Además de realizar un cuestionario de preguntas por cada proceso en base a las actividades, se coordinó con anticipación con la UTIC la entrega de información necesaria, para posteriormente validar toda la documentación facilitada. Anexo (Tabla12).

En el presente proyecto de tesis se realizó el estudio sobre los cuatro procesos más críticos en base al análisis realizado en el dominio Construir, Adquirir e Implementar, a continuación el detalle de los procesos y sus prácticas de gestión:

BAI01 Gestionar los programas y Proyectos (BAI01.01 Mantener un enfoque estándar para la gestión de programas y proyectos, BAI01.02 Iniciar un programa, BAI01.03 Gestionar el compromiso de las partes interesadas, BAI01.04 Desarrollar y mantener el plan de programa, BAI01.05 Lanzar y ejecutar el programa, BAI01.06 Supervisar, controlar e informar de los resultados del programa, BAI01.07Lanzar e iniciar proyectos dentro de un programa, BAI01.08 Planificar proyectos, BAI01.09Gestionar la calidad de los programas y proyectos, BAI01.10 Gestionar el riesgo de los programas y proyectos, BAI01.11 Supervisar y controlar proyectos, BAI01.12 Gestionar los recursos y los paquetes de trabajo del Proyecto, BAI01.13 Cerrar un proyecto o iteración, BAI01.14 Cerrar un programa. El proceso en mención fue analizado en función del cuestionario No. 1.

BAI02 Gestionar la definición de requisitos (BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio, BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas, BAI02.03 Gestionar los riesgos de los requerimientos, BAI02.04 Obtener la aprobación de los

requerimientos y soluciones. El proceso en mención fue analizado en función del cuestionario No. 2.

BAI04 Gestionar la Disponibilidad y la Capacidad (BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia, BAI04.02 Evaluar el impacto en el negocio, BAI04.02 Evaluar el impacto en el negocio, BAI04.03 Planificar requisitos de servicio nuevos o modificados, BAI04.04 Supervisar y revisar la disponibilidad y la capacidad. El proceso en mención fue analizado en función del cuestionario No. 3.

BAI06 Gestionar los Cambios (BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio, BAI06.02 Gestionar cambios de emergencia, BAI06.03 Hacer seguimiento e informar de cambios de estado, BAI06.04 Cerrar y documentar los cambios. El proceso en mención fue analizado en función del cuestionario No. 4.

Tabla 12
Plan de Investigación de Campo

PLAN DE INVESTIGACIÓN DE CAMPO

METAS TI	METAS DE PROCESO	PRACTICA DE GESTION					ACTIVIDADES	DOCUMENTACIÓN DE REFERENCIA	Temas Importantes	FUENTE MATRIZ RACI	Observaciones o Coordinaciones
		DESCRIPCION	VIENE DESDE	ENTRADAS	SALIDAS	SALE A					
01 Alineamiento de TI y la estrategia de negocio 04 Riesgos de negocio relacionados con las TI gestionados 05 Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI 13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	1. Las partes interesadas relevantes están comprometidas con los programas y los proyectos.	BAI01.01 Mantener un enfoque estándar para la gestión de programas y proyectos.	EDM02.02	Requisitos para revisiones de cambio de estado (stage-gate)	Enfoques actualizados de gestión de programas y proyectos.	Interno	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. Asegurar que el enfoque cubra todo el ciclo de vida y las disciplinas a utilizar, incluyendo la gestión de alcance, recursos, riesgos, costes, calidad, tiempo, comunicaciones, involucración de las partes interesadas, adquisiciones, control de cambios, integración y generación de beneficios.	Requisitos para revisiones de cambio de estado (stage-gate)	Enfoque estándar de gestión de programas, proyectos y buenas prácticas basadas en procesos definidos y el uso de tecnología apropiada	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	2. El alcance y los resultados de los programas y proyectos son viables y están alineados con los objetivos.	BAI01.02 Iniciar un programa.	APO03.04	• Descripciones en fase de implementación. • Requisitos de recursos	Caso de negocio de concepto del programa	APO05.03	2. 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.	• Descripciones en fase de implementación•Requisitos de recursos	confirmación de mandato de programa con los patrocinadores y las partes interesadas	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

3. Los planes de programas y proyectos tienen probabilidades de lograr los resultados esperados.				4. 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.	Plan de realización de beneficios	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
4. Las actividades de los programas y proyectos se ejecutan de acuerdo a los planes.				5. 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.	Aprobación preliminar el caso de negocio inicial y toma de decisiones	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
5. Existen suficientes recursos de los programas y proyectos para realizar las actividades de acuerdo a los planes.				6. Designar un gerente dedicado para el programa, con las competencias y habilidades adecuadas para gestionar el programa de forma eficiente y efectiva.	designación de responsable	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
6. Los beneficios esperados de los programas y proyectos son obtenidos y aceptados.	BAIO01.03 Gestionar el compromiso de las partes interesadas.		• Plan de involucración de las partes interesadas • Resultados de la evaluación de efectividad del compromiso de las partes interesadas	Interno	1. 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.	Planificación de partes interesadas internas y externas	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

	BAI01.04 Desarrollar y mantener el plan de programa.	APO05.03	Programas seleccionados con hitos de ROI	Plan de programa	Interno	1. 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, así como las reestructuraciones organizacionales necesarias para lograr los resultados que la empresa espera del programa.	Programas seleccionados con hitos de ROI	Documentación de planes de todos los proyectos	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		APO07.03	Matriz de habilidades y competencias	Presupuesto del programa y registro de beneficios	APO05.06 APO06.05	2. 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. Especificar las bases para la contratación y asignación de miembros del personal competentes y/o contratistas a los proyectos. Definir los roles y las responsabilidades para todos los miembros del equipo y otras partes interesadas.	Matriz de habilidades y competencias	Habilidades y recursos para ejecutar proyectos	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		APO07.05	Inventario de recursos humanos de TI y del negocio	Requerimientos de recursos y roles	APO07.05 APO07.06	3. 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	Inventario de recursos humanos de TI y del negocio	Responsabilidades ejecutivas para cada proyecto	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

						actividades de los proyectos.				
		BAI05.02	Equipo y roles para la implementación			5. 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.	Equipo y roles para la implementación	Plan de programa actualizado para alineamiento de objetivos estratégicos	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		BAI05.03	Plan de comunicación de la visión							
		BAI05.04	Identificación de logros rápidos (quick wins)							
		BAI07.03	Plan de pruebas de aceptación aprobado							
		BAI07.05	Aceptación y pase a producción aprobados							
	BAI01.05 Lanzar y ejecutar el programa.	BAI05.03	Comunicaciones de la visión	Resultados de la supervisión de la realización de beneficios	APO05.06 APO06.05	1. Planificar, dar recursos y asignar las responsabilidades requeridas para los proyectos necesarios para logar los resultados del programa, basados en las revisiones de financiación y las aprobaciones en cada revisión de cambio de fase (stage-gate).	Comunicaciones de la visión	Roles y responsabilidades en los proyectos	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
				Resultados de la supervisión del logro de metas del programa	APO02.04	2. 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		Etapas del proceso de desarrollo, Funcionalidad, rendimiento y calidad	R:Jefe Lab A:Director DECC C:Director TH I:	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

						interesadas. Después de la finalización exitosa de la revisión de funcionalidad, rendimiento y calidad, y antes de finalizar las actividades de la etapa, obtener la aprobación formal y la firma de todas las partes.			Vicerrector Adm	
				Planes de auditoría del programa	MEA02.06	4. Administrar cada programa o proyecto para asegurar que la toma de decisiones y las actividades de entrega están enfocadas en el valor mediante la consecución de los beneficios y las metas del negocio de una manera consistente, considerando el riesgo y alcanzando los requerimientos de las partes interesadas.		Administración de programa o proyecto, Beneficios y metas del negocio.	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	BAI01.06 Supervisar, controlar e informar de los resultados del programa.	EDM02.03	Realimentación sobre el rendimiento del portafolio y del programa	Resultado de la revisión del rendimiento del programa	MEA01.03	1. Supervisar y controlar el rendimiento del programa general y de los proyectos dentro del programa, incluyendo la contribución al negocio y a TI de los del usuario, controles internos y aceptación de responsabilidades.	Realimentación sobre el rendimiento del portafolio y del programa	Supervisar y controlar el rendimiento de programas y proyectos	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		APO05.02	Expectativas del retorno de la inversión	Resultados de revisiones en los cambios de fase (stage-gate)	EDM02.01 APO02.04 APO05.04	2. Supervisar y controlar el desempeño versus las estrategias y metas de la organización y TI e informar a la dirección de la organización de los cambios implementados, los beneficios logrados versus el plan y la idoneidad del proceso de obtención de beneficios.	Expectativas del retorno de la inversión	Desempeño versus estrategia y metas	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

	APO05.03	Evaluación de los casos de negocio	3. Supervisar y controlar los servicios, activos y recursos de TI creados o modificados como resultado del programa. Verificar las fechas de implementación y puesta en servicio. Informar a la dirección de los niveles de rendimiento, entrega de servicio sostenido y contribución al valor.	Evaluación de los casos de negocio	servicios, activos y recursos de TI	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	APO05.04	Informes del desempeño del portafolio de inversiones	6. Actualizar los portafolios operacionales de TI que reflejen los cambios que resultan de los programas en los portafolios relevantes de servicios.	Informes del desempeño del portafolio de inversiones	Portafolios operacionales de TI	R:Jefe Lab A:Director DECC C:Director TH I	Coordinar entrega cuestionario Director de la UTIC
	APO05.06	• Acciones correctivas para mejorar la realización de beneficios. • Resultados de beneficios y comunicaciones relacionadas		• Acciones correctivas para mejorar la realización de beneficios. • Resultados de beneficios y comunicaciones relacionadas			
	APO07.05	• Registro de uso de recursos. • Análisis de escasez de recursos		• Registro de uso de recursos. • Análisis de escasez de recursos			
	BAI05.04	Comunicación de beneficios		Comunicación de beneficios			
	BAI06.03	Informes de estado de solicitudes de cambios		Informes de estado de solicitudes de cambios			
	BAI07.05	Evaluación de los resultados de aceptación		Evaluación de los resultados de aceptación			

CONTINÚA →

BAI01.07 Lanzar e iniciar proyectos dentro de un programa.		Declaraciones de alcance de proyecto	Interno	1. Crear un entendimiento común del alcance del proyecto entre las partes interesadas, proveer a las partes interesadas de una declaración clara y por escrito que defina la naturaleza, alcance y beneficio de cada proyecto.	Alcance del proyecto entre las partes interesada	Alcance del proyecto entre las partes interesada?	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		Definiciones de proyecto	Interno	3. Asegurar que las partes interesadas y patrocinadores claves dentro de la organización y TI estén de acuerdo y acepten los requerimientos de los proyectos, incluyendo la definición del criterio de éxito del proyecto (aceptación) y los indicadores claves de desempeño (KPIs).		Partes interesadas y patrocinadores claves dentro de la organización y TI	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
				6. Hacer un seguimiento de la ejecución del proyecto, poniendo mecanismos tales como informes regulares y revisiones de cambios de estado (stagegate), lanzamientos o fases de una manera oportuna y con una aprobación adecuada.		Seguimiento de la ejecución del proyecto	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

	BAI01.08 Planificar proyectos.	BAI07.03	Plan aprobado de aceptación de pruebas	Planes del proyecto	Interno	1. Desarrollar un plan de proyecto que provea información que permita a la dirección controlar el progreso del proyecto progresivamente. El plan debería incluir detalles de los entregables del proyecto y criterios de aceptación, recursos y responsabilidades requeridas interna y externamente, estructuras claras de división de trabajo y paquetes de tareas, estimaciones de recursos necesarios, hitos/planes de lanzamiento/fases, dependencias claves y la identificación del camino critico (critical path).		Plan de proyecto, entregables, recursos y responsabilidades	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
				Línea de referencia (baseline) del proyecto		2. Mantener el plan del proyecto y cualquier plan dependiente (por ejemplo, plan de riesgo, plan de calidad, plan de obtención de beneficios) para asegurar que están actualizados y reflejan su progreso real y los cambios materiales aprobados.	Plan aprobado de aceptación de pruebas	Plan de riesgo, plan de calidad, plan de obtención de beneficios	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
				Informes y comunicaciones del proyecto		5. Asegurarse que cada hito es acompañado por un entregable significativo que requiere revisión y aprobación.		Hito	R:Jefe Lab A:Director DECC C:Director TH	Coordinar entrega cuestionario Director de la UTIC
						6. Establecer un marco base del proyecto (por ejemplo, coste, cronograma, alcance, calidad) que es debidamente revisado, aprobado e incorporado en el plan de proyectos integrado.		Marco Base	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

	BAI01.09 Gestionar la calidad de los programas y proyectos.	APO11.01	Plan de gestión de la calidad	Plan de gestión de la calidad	BAI02.04 BAI03.06 BAI07.01	1. Identificar las actividades y prácticas de aseguramiento para apoyar la acreditación sistemas nuevos o modificados durante la planificación del programa y del proyecto e incluirlos dentro de los planes integrados. Asegurarse que las tareas provean garantías de que las soluciones de seguridad y los controles internos cumplen con los requerimientos definidos.	Plan de gestión de la calidad	Actividades y practicas	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		APO11.03	Requisitos de cliente para la gestión de la calidad	Requerimientos para la verificación independiente de los entregables	BAI07.03	2. Proporcionar garantías de calidad para los entregables del proyecto, identificar a propietarios y responsabilidades, revisar el proceso de calidad, criterios de éxito y las métricas de desempeño.	Requisitos de cliente para la gestión de la calidad	Garantías de calidad, propietarios y responsabilidades	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	BAI01.10 Gestionar el riesgo de los programas y proyectos.	APO12.02	Resultados del análisis de riesgo	Plan de gestión de riesgos del proyecto	Interno	1. Establecer un enfoque de gestión de riesgo de proyectos alineado con el marco de referencia de ERM. Asegurar que este enfoque incluya la identificación, análisis, respuesta, mitigación, supervisión y control del riesgo.	Resultados del análisis de riesgo	Enfoque de gestión	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		BAI02.03	• Acciones de mitigación de riesgos. • Registro de requisitos de riesgos	Resultados de la evaluación de riesgos del proyecto	Interno	2. Asignar la responsabilidad para ejecutar el proceso de gestión del riesgo de los proyectos de la entidad al personal con las capacidades adecuadas y asegurar que está incorporado en las prácticas de desarrollo de la solución. Considerar asignar este perfil a un equipo independiente.	• Acciones de mitigación de riesgos. • Registro de requisitos de riesgos	Responsabilidades, capacidades adecuadas, prácticas de desarrollo	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

		Fuera del Ámbito de COBIT	Marco de referencia de ERM	Registro de riesgos del proyecto	Interno	3. Realizar un análisis de riesgo del proyecto para identificar y cuantificar el riesgo de manera continua durante el proyecto. Gestionar y comunicar el riesgo adecuadamente dentro de la estructura de gobierno del proyecto.	Marco de referencia de ERM	Análisis de riesgos	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
						4. Reevaluar el riesgo del proyecto periódicamente, incluyendo al inicio de cada fase de un proyecto importante y como parte de las evaluaciones de solicitudes de cambios importantes.		Evaluaciones solicitudes de cambios	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	BAI01.11 Supervisar y controlar proyectos.			Criterios de desempeño del proyecto	Interno	3. Notificar el progreso del proyecto dentro del programa, las desviaciones de los criterios claves de desempeño, establecidos y los efectos positivos y negativos en los programas y en los proyectos que los componen a las partes interesadas identificadas como claves.	Criterios de desempeño del proyecto	Proyecto del programa, desviaciones de criterios	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
				Informes del avance del proyecto	Interno	4. Supervisar los cambios al programa y revisar los criterios claves de desempeño del proyecto para determinar si estos representan medidas válidas del avance.	Informes del avance del proyecto	Supervisar programa, criterios claves de desempeño	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
				Cambios acordados al proyecto	Interno	5. Documentar y enviar cualquier cambio al programa a las partes interesadas claves antes de su adopción. Comunicar los criterios revisados a los jefes de proyecto para su uso en los informes futuros de desempeño.	Cambios acordados al proyecto	Comunicación de criterios revisados	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

			6. Recomendar y supervisar las acciones correctivas, cuando sean requeridas, en línea con el marco de gobierno de programas y proyectos.	Recomendar y supervisar	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto.	Requerimientos de recursos del proyecto	APO07.05 APO07.06	1. Identificar las necesidades de recursos del negocio y TI para el proyecto y mapear claramente los perfiles y responsabilidades, con las responsabilidades para el escalado y la toma de decisiones que han sido acordadas y entendidas.	Necesidades de recursos, responsabilidades y toma de decisiones	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	Roles y responsabilidades del proyecto	Interno	2. Identificar los requerimientos de habilidades y tiempo para todos los individuos involucrados en las fases del proyecto con relación a sus perfiles definidos. Asignar personal a los roles basándose en la información sobre las habilidades disponibles (p.ej. matriz de habilidades de TI).	Identificar requerimientos, habilidades	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	Diferencias en la planificación del proyecto	Interno	4. Considerar y definir claramente los roles y responsabilidades de otras partes involucradas, incluyendo financiero, legal, compras, RRHH, auditoría interna y cumplimiento.	Roles y responsabilidades	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
			6. Identificar y autorizar la ejecución del trabajo de acuerdo al plan de proyecto.	Identificar y autorizar	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA →

BAI01.13 Cerrar un proyecto o iteración.			Resultados de la revisión post-implementación	APO02.04	2. Planificar y ejecutar revisiones post-implementación para determinar si los proyectos entregaron los beneficios esperados y para mejorar la metodología de gestión de proyecto y el proceso de desarrollo de sistemas.		Planificar y ejecutar revisiones post implementación	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	BAI07.08	• Plan de acciones de remediación. • Informe de revisión post-implementación	Lecciones aprendidas del proyecto	Interno	3. Identificar, asignar, comunicar y rastrear las actividades incompletas necesarias para lograr los resultados y beneficios planeados del programa del proyecto.	• Plan de acciones de remediación. • Informe de revisión post-implementación	Identificar, asignar, comunicar y rastrear	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
			Confirmaciones de aceptación de las partes interesadas del proyecto	Interno					
BAI01.14 Cerrar un programa.	BAI07.08	• Plan de acciones de remediación. • Informe de revisión post implementación	Comunicación del retiro del programa y rendición de cuentas en curso	APO05.05 APO07.06	1. Llevar el programa a un cierre ordenado, incluyendo una aprobación formal, desmantelamiento de la organización del programa y la función de apoyo, validación de los entregables y comunicación de la retirada.	• Plan de acciones de remediación. • Informe de revisión post implementación	Cierre ordenado, aprobación desmantelamiento	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
					2. Revisar y documentar las lecciones aprendidas. Una vez que el programa ha sido retirado, elimínelo del portafolio de inversiones activas.		Revisión y documentación	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

01 Alineamiento de TI y estrategia de negocio 07 Entrega de servicios de TI de acuerdo a los requisitos del negocio 12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	1. Los requerimientos funcionales y técnicos del negocio reflejan las necesidades y expectativas de la organización.	BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio.	APO01.06	• Procedimientos de integridad de datos • Guías de control y seguridad de los datos • Guías de clasificación de datos	Repositorio de definición de requerimientos	BAI03.01 BAI03.02 BAI04.01 BAI05.01	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, reconociendo que los requerimientos pueden cambiar y llegar a ser más detallados según se implementen.	• Procedimientos de integridad de datos • Guías de control y seguridad de los datos • Guías de clasificación de datos	Requerimientos de partes interesadas?	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	2. La solución propuesta satisface los requerimientos funcionales, técnicos y de cumplimiento del negocio.		APO03.01	Principios de arquitectura	Confirmación de los criterios de aceptación de las partes interesadas	BAI03.01 BAI03.02 BAI04.03 BAI05.01 BAI05.02	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.	Principios de arquitectura	Requerimientos técnicos y funcionales.	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	3. El riesgo asociado con los requerimientos ha sido tomado en cuenta en la solución propuesta.		APO03.02	• Modelo de arquitectura de la información • Descripciones de los dominios de referencia y definición de arquitectura	Registro de las peticiones de cambios de los requerimientos	BAI03.09	7. Hacer seguimiento y controlar el alcance, los requerimientos y los cambios a lo largo del ciclo de vida de la solución durante el proyecto según evolucione la comprensión de la solución.	• Modelo de arquitectura de la información • Descripciones de los dominios de referencia y definición de arquitectura	Seguimiento, alcance, cambios	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

4. Los requerimientos y soluciones propuestas cumplen con los objetivos del caso de negocio (valor esperado y costes probables).		APO03.05 APO10.02 APO11.03	Guía de desarrollo de la solución RFIs y RFPs de proveedores Criterios de aceptación				Guía de desarrollo de la solución RFIs y RFPs de proveedores Criterios de aceptación			
	BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas.	APO03.05	Guía de desarrollo de la solución	Informe de estudio de viabilidad	BAI03.02 BAI03.03	1. 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.	Guía de desarrollo de la solución	Estudio de viabilidad	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		APO10.01	Catálogo de proveedores	Plan de alto nivel de adquisiciones/ desarrollo	APO10.02 BAI03.01	2. 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.	Catálogo de proveedores	Adquisición o desarrollo de la solución	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		APO10.02	• Resultados de decisión de las evaluaciones de proveedores • Evaluaciones de RFI y RFP • RFIs y RFPs de proveedores			3. Revisar las soluciones alternativas con todas las partes interesadas y seleccionar la más apropiada basada en criterios de viabilidad, incluyendo costes y riesgos.	• Resultados de decisión de las evaluaciones de proveedores • Evaluaciones de RFI y RFP • RFIs y RFPs de proveedores	soluciones alternativas	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

	APO11.03	Criterios de aceptación				Criterios de aceptación			
	BAI02.03 Gestionar los riesgos de los requerimientos.		Registro de riesgos de los requerimientos	BAI01.10 BAI03.02 BAI04.01 BAI05.01	1. 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).		Requerimientos técnicos, funcionales, de calidad y riesgos relativos al procesamiento de la información	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
			Acciones de mitigación de riesgos	BAI01.10 BAI03.02 BAI05.01	2. Analizar y priorizar los riesgos de los requerimientos conforme probabilidad e impacto. Si aplica, determinar los impactos en coste y tiempo.		Analizar y priorizar	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
					3. Identificar modos de controlar, evitar o mitigar los riesgos de los requerimientos en orden de prioridad.		Controlar, evitar o mitigar los riesgos de los requerimientos	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

		BAI02.04 Obtener la aprobación de los requerimientos y soluciones.	BAI01.09	Plan de gestión de calidad	Aprobaciones del patrocinador de los requerimientos y soluciones propuestas	BAI03.02 BAI03.03 BAI03.04	1. Asegurar que el patrocinador de negocio o propietario del producto toman la decisión final con respecto a la elección de la solución, enfoque de adquisición y diseño de alto nivel acorde al caso de negocio. Coordinar la realimentación de las partes interesadas afectadas y obtener el cierre por parte de las autoridades apropiadas tanto técnicas como de negocio (por ejemplo, dueño del proceso, arquitecto de empresa, gestor de operaciones, seguridad) para el enfoque propuesto.	Plan de gestión de calidad	Propietario del producto, realimentación de partes interesadas	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
					Aprobación de las revisiones de calidad	APO11.02	2. 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.		Revisiones de calidad	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio 11 Optimización de activos, recursos y capacidades de TI 14 Disponibilidad de información útil y relevante	1. El plan de disponibilidad anticipa la expectativa del negocio en cuanto a requerimientos críticos de capacidad	BAI04.01 Evaluar la disponibilidad ,rendimiento y capacidad actual y crear una línea de referencia.	BAI02.01	Repositorio de definición de requisitos	Líneas de referencia de disponibilidad, rendimiento y capacidad	Interno	2. Supervisar el rendimiento y la utilización de la capacidad reales frente a los umbrales definidos, con el apoyo cuando sea necesario de software automatizado.	Repositorio de definición de requisitos	Rendimiento y la utilización de la capacidad reales	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	2. Cumplimiento de requerimientos de capacidad, rendimiento y disponibilidad		BAI02.03	Registro de requisitos de riesgo	Evaluaciones respecto a ANSs	APO09.05	3. Identificar y dar seguimiento a todos los incidentes causados por un rendimiento o una capacidad inadecuados.	Registro de requisitos de riesgo	Seguimiento, incidencias	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

para la toma de decisiones	3. Cuestiones de disponibilidad, rendimiento y capacidad identificados y resueltos de manera rutinaria					4. Evaluar periódicamente los niveles reales de rendimiento a todos los niveles de procesamiento (la demanda del negocio, capacidad de servicio y capacidad de los recursos) mediante la comparación con las tendencias y los ANSs, teniendo en cuenta los cambios en el entorno.		Niveles reales de rendimiento	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		BAI04.02 Evaluar el impacto en el negocio.			Escenarios de disponibilidad, rendimiento y capacidad	Interno	2. Realizar un mapa de las soluciones o servicios seleccionados con la(s) aplicación(es) e infraestructura (TI y de instalaciones) de los que dependen, para permitir un enfoque en los recursos críticos para la planificación de la disponibilidad.		Mapa de soluciones	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
			BAI03.02	ANSs internos y externos	Evaluaciones de impacto en el negocio de disponibilidad, rendimiento y capacidad	Interno	3. Recolectar datos de patrones de disponibilidad de los registros de fallos pasados y de la monitorización del rendimiento. Utilizar herramientas de modelado que ayuden a predecir fallos basados en tendencias de utilización en el pasado y expectativas de la dirección sobre nuevos entornos o condiciones de los usuarios.	ANSs internos y externos	Recolección de datos	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
							4. Crear escenarios basados en datos recolectados, describiendo situaciones de disponibilidad futura para ilustrar varios niveles de capacidad potenciales necesarios para alcanzar el objetivo de rendimiento de la disponibilidad.	ANSs internos y externos	Datos recolectados	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

						7. Asegurar que los propietarios de procesos de negocio comprenden completamente y están de acuerdo con los resultados del análisis. Obtener una lista de escenarios de riesgo inaceptables de los propietarios de negocio que requieran una respuesta para reducir el riesgo a niveles aceptables.		propietarios de procesos de negocio	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	BAI04.03 Planificar requisitos de servicio nuevos o modificados.	BAI02.01	Criterios de aceptación confirmados de las partes interesadas	Mejoras priorizadas	APO02.02	2. Identificar las implicaciones en la disponibilidad y la capacidad de cambios en las necesidades del negocio y oportunidades de mejora. Utilizar técnicas de modelado para validar los planes de disponibilidad, rendimiento y capacidad.	Criterios de aceptación confirmados de las partes interesadas	Disponibilidad y la capacidad de cambios en las necesidades del negocio	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		BAI03.01	Especificaciones de diseño de alto nivel aprobadas			3. Priorizar las necesidades de mejora y crear planes de disponibilidad y capacidad justificables en costes.	Especificaciones de diseño de alto nivel aprobadas	Necesidades de mejora	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		BAI03.02	Especificaciones de diseño detallado aprobadas	Planes de capacidad y rendimiento	APO02.02	5. Asegurar que la dirección lleva a cabo comparaciones de la demanda actual de recursos con la demanda y suministro previstos para evaluar las técnicas de previsión actuales y realizar mejoras donde sea posible.	Especificaciones de diseño detallado aprobadas	Recursos con la demanda y suministro previstos	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		BAI03.03	Componentes de la solución documentados				Componentes de la solución documentados			

CONTINÚA

		BAI04.04 Supervisar y revisar la disponibilidad y la capacidad.			Informes de disponibilidad y rendimiento	MEA01.03	2. Proporcionar información periódica de los resultados en una forma apropiada para su revisión por las TI y la gestión del negocio y comunicar a la dirección empresarial.		Información periódica de los resultados	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
							3. Integrar las actividades de supervisión e información en las actividades iterativas de gestión de la capacidad (supervisión, análisis, ajuste e implementaciones).		Actividades de supervisión e información	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
							4. Proveer informes de capacidad para los procesos de presupuesto.		Informes de capacidad	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
04 Riesgos de negocio relacionados con las TI gestionados 07 Entrega de servicios de TI de acuerdo a los requisitos del negocio 10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	1. Los cambios autorizados son realizados de acuerdo a sus cronogramas respectivos y con errores mínimos.	BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio.	BAI03.05	Componentes de la solución integrados y configurados	Evaluaciones de impacto	Internal	1. Utilizar peticiones de cambio formales para posibilitar que los propietarios de procesos de negocio y TI soliciten cambios en procesos de negocio, infraestructura, sistemas o aplicaciones. Asegurar que todos estos cambios surgen solo a través del proceso de gestión de las peticiones de cambio.	Componentes de la solución integrados y configurados	Peticiones de cambio formales	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	2. Las evaluaciones de impacto revelan el efecto de los cambios sobre todos los componentes afectados.		DSS02.03	Peticiones de servicio aprobadas	Peticiones de cambio aprobadas	BAI07.01	3. Priorizar todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio, recursos necesarios, así como las razones contractuales, legales o de regulación que motivan el cambio.	Peticiones de servicio aprobadas	Peticiones de cambio sobre la base de los requisitos técnicos y de negocio	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

3. Todos los cambios de emergencia son revisados y autorizados una vez hecho el cambio.		DSS03.03	Soluciones propuestas para errores conocidos			4. Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio (BCPs) y proveedores de servicios para asegurar que todos los componentes afectados	Soluciones propuestas para errores conocidos	Infraestructura, sistemas y aplicaciones, planes de continuidad de negocio	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
4. Las principales partes interesadas están informadas sobre todos los aspectos del cambio.		DSS03.05	Soluciones sostenibles identificadas			5. Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser pre-aprobados como cambios estándar.	Soluciones sostenibles identificadas	Gestores de servicio, partes interesadas de los departamentos de TI	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		DSS04.08	Cambios aprobados a los planes	Plan de cambio y cronograma	BAI07.01	6. Planificar y programar todos los cambios aprobados.	Cambios aprobados a los planes	Planificar y programar	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		DSS06.01	Análisis de causas raíz y recomendaciones				Análisis de causas raíz y recomendaciones			
	BAI06.02 Gestionar cambios de emergencia.			Revisión de cambios de emergencia tras su implementación	Interno	1. Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.		Procedimiento documentado	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

						2. Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se ha aplicado el cambio.	Accesos de emergencia	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
						3. Supervisar todos los cambios de emergencia y realizar revisiones post-implantación involucrando a todas las partes interesadas. La revisión debería considerar e iniciar acciones correctivas basadas en causas raíz tales como problemas en los procesos de negocio, desarrollo y mantenimiento de sistemas de aplicación, entornos de desarrollo y pruebas, documentación y manuales e integridad de datos.	cambios de emergencia	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
						4. Definir qué constituye un cambio de emergencia.	Definir un cambio de emergencia	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	BAI06.03 Hacer seguimiento e informar de cambios de estado.	BAI03.09	Registro de todas las peticiones de cambio aprobadas, y aplicadas	Reporte del estado de cambio de una petición	BAI01.06 BAI10.03	1. Categorizar las peticiones de cambio en el proceso de seguimiento (ej. rechazados, aprobados pero aún no iniciados, aprobados y en proceso y cerrados).	Peticiones de cambio	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

				2. Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado global (ej. análisis de antigüedad de las peticiones de cambio). Asegurar que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre.	informes de cambios de estado	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
				3. Supervisar los cambios abiertos para asegurar que los cambios aprobados son cerrados en los plazos previstos, de acuerdo a su prioridad.	cambios abiertos	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
				4. Mantener un sistema de seguimiento e informe para todas las peticiones de cambio.	Informe para todas las peticiones de cambio	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
	BAI06.04 Cerrar y documentar los cambios.	Documentación del cambio	Interno	1. Incluir los cambios en la documentación (ej. procedimientos de negocio y operativos de TI, documentación de continuidad de negocio y recuperación frente a desastres, información de configuración, documentación de la aplicación, pantallas de ayuda y material de formación) en el procedimiento de gestión del cambio.	Procedimientos de negocio y operativos de TI	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

CONTINÚA

		2. Definir un periodo apropiado de conservación de la documentación del cambio, la documentación del sistema antes y después del cambio y la documentación de usuario.	Documentación del sistema antes y después del cambio	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC
		3. Someter a la documentación a la misma revisión que al cambio en sí mismo.	documentación a la misma revisión	R:Jefe Lab A:Director DECC C:Director TH I: Vicerrector Adm	Coordinar entrega cuestionario Director de la UTIC

Fuente: UTIC (2014)

3.5 Elaboración de Instrumentos de investigación de campo

Para el plan de investigación de campo o programa de auditoría se utilizó recursos humanos, evidencia (encuestas o cuestionarios) y equipos tecnológicos.

- Recurso Humano: Grupo de auditores que recopila y analiza la información, aplicando una metodología de auditoría basado en el modelo COBIT y su aplicación.
- Recursos de Evidencia: El programa de auditoría que se ha planificado, parte de la elaboración de una Matriz de Riesgos TI, para identificar los procesos y actividades más críticos y así dar paso al plan de investigación de campo que se respaldará con :
- Cuestionarios: la información obtenida a través de él, nos permite adelantar un pre diagnóstico de la situación de la unidad y orienta el trabajo de campo.
- Observación directa: técnica que permite observar la realidad de la organización y puede ser de dos tipos, no participante es aquella en que el auditor observa externamente el proceso sin interferir en ellos y participante es aquella en la que el auditor participa en los procesos de la unidad auditada, sea integrándose en el grupo y sus actividades
- Recurso Tecnológico: Computadora portátil, utilizada para la documentación y almacenamiento de la información entregada por la UTIC.
- Software, programas de ofimática (Word, Excel, power point, etc) que servirán de apoyo para la elaboración del proyecto de auditoría.

3.6 Aplicación de Instrumentos de investigación de campo

Para poder materializar las técnicas antes mencionadas se ha dotado de instrumentos de investigación tales como: cuestionarios, observación directa, programas informáticos, etcétera.

3.7 Análisis de la información

Informe Detallado

El Informe Detallado, que consta en el Capítulo 4, fue presentado para su revisión el día lunes 4 de Abril del 2015 al Ing. Rubén Arroyo, Director del proyecto de tesis de la Universidad de las Fuerzas Armadas (ESPE)

Informe Final/Ejecutivo

Una vez revisado el Informe Detallado y aceptadas las respectivas recomendaciones y puntos de vista, se procederá a presentar el Informe Final/Ejecutivo.

CAPITULO IV. INFORME FINAL

4.1 Informe Ejecutivo.

4.1.1 Antecedentes

El proyecto de tesis Evaluación Técnica Informática de la Adquisición e Implementación de la ESPE Sede Principal. Fue concebido por análisis de la realidad actual de la institución. Proyecto que fue aprobado por la junta de posgrados y ejecutado en la UTIC como proyecto de tesis.

Estudio de proyecto que radica en realizar una evaluación técnica informática de la adquisición e implementación de la ESPE Sede Principal. Basado en el marco de referencia COBIT 5, con el fin de identificar las vulnerabilidades y emitir las recomendaciones para mitigar los riesgos en la institución.

La evaluación técnica informática de la Adquisición e Implementación de la ESPE Sede Principal va dirigida a las UTIC, con el objetivo de recomendar controles para fortalecer a la unidad tecnológica.

4.1.2 Descripción Metodológica

El proyecto de tesis fue realizado en el dominio Construir, adquirir e implementar del modelo de referencia COBIT 5, Dominio que fue analizado y desarrollado por el grupo de auditores, integrado por dos maestrantes y orientados por dirigentes del proyecto “Docentes de la Escuela Politécnica del Ejército”.

El desarrollo del presente proyecto de tesis cubrió aspectos de gestión de programas y proyectos, gestión de definición de requisitos, gestión de disponibilidad y capacidad, y gestión de cambios. Con el objetivo de determinar los riesgos potenciales a la que se encuentra sometida la institución.

Herramientas adicionales a la del modelo de referencia COBIT 5, se utilizó herramientas de implementación para la recolección de la información como:

- Reunión con el personal de la UTIC.
- Investigación documental de los procedimientos, actividades, proyectos, programas, registros, planificaciones, matrices y catálogos de proyectos.

Luego de la etapa de recolección de información se procedió a realizar el análisis de presentación de resultados, donde los funcionarios de la UTIC y los involucrados directos con los procesos de adquisición e implementación recibieron el informe de auditoría con las observaciones, criterios, condiciones, causas y efectos hallados en el análisis, documento donde se redacta las recomendaciones respectivas para la aplicación en la institución.

4.1.3 Principales hallazgos

En base al análisis y evaluación de la realidad actual de la adquisición e implementación de la ESPE Sede principal, se han detectados falencias importantes que se detallan a continuación.

DOMINIO CONSTRUIR, ADQUIRIR E IMPLEMENTAR

- Director de la UTIC, debe realizar una guía estandarizada para la gestión de programas y proyectos basada en buenas prácticas, la que estará sujeta a una mejora continua y procesos definidos, el cual debe ser evaluado periódicamente para fortalecer la gestión de programas y proyectos.
- Administrador de Contrato, debe 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
- Administrador de Contrato, debe 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, así como las reestructuraciones organizacionales necesarias para lograr los resultados que la empresa espera del programa.

- Administrador de Contrato, debe planificar, dar recursos y asignar las responsabilidades requeridas para los proyectos necesarios para logar los resultados del programa, basados en las revisiones de financiación y las aprobaciones en cada revisión de cambio de fase (stage-gate).
- Administrador de Contrato, debe supervisar y controlar el rendimiento del programa general y de los proyectos dentro del programa, incluyendo la contribución al negocio y a TI de los proyectos, e informar de una manera oportuna, completa y veraz. Los informes pueden incluir cronogramas, financiación, funcionalidad, satisfacción del usuario, controles internos y aceptación de responsabilidades.
- Administrador de Contrato, debe crear un entendimiento común del alcance del proyecto entre las partes interesadas, proveer a las partes interesadas de una declaración clara y por escrito que defina la naturaleza, alcance y beneficio de cada proyecto.
- Director de la UTIC, debe establecer un marco base del proyecto (por ejemplo, coste, cronograma, alcance, calidad) que es debidamente revisado, aprobado e incorporado en el plan de proyectos integrado.
- Directo de la UTIC, debe realizar un análisis de riesgo del proyecto para identificar y cuantificar el riesgo de manera continua durante el proyecto. Gestionar y comunicar el riesgo adecuadamente dentro de la estructura de gobierno del proyecto.
- Director de la UTIC, debe Planificar y ejecutar revisiones post-implementación para determinar si los proyectos entregaron los beneficios esperados y para mejorar la metodología de gestión de proyecto y el proceso de desarrollo de sistemas

- Administrador de contrato: Elaborar 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
- Administrador de contrato, debe evaluar periódicamente los niveles reales de rendimiento a todos los niveles de procesamiento (la demanda del negocio, capacidad de servicio y capacidad de los recursos) mediante la comparación con las tendencias y los ANSs, teniendo en cuenta los cambios en el entorno.
- Administrador de contrato, de proporcionar información periódica de los resultados en una forma apropiada al director de la UTIC, autoridad que en base a la información facilitada tomará decisiones para la mejora de los procesos.
- Administrador de contrato, debe elaborar políticas y procedimientos para priorizar todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio, recursos necesarios, así como las razones contractuales, legales o de regulación que motivan el cambio.
- Administrador de contrato, se debe elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios, asegurando que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre.

4.1.4 Conclusión

Para está evaluación técnica informática se realizó la implementación del modelo de referencia COBIT 5, estándar para fortalecer los procesos y actividades de la ESPE sede principal. Institución donde se realizó el análisis de

riesgos más críticos a los que se expone la ESPE, permitiendo detectar las vulnerabilidades en los procesos y actividades de la adquisición e implementación que gestiona la UTIC, lo que permitió emitir recomendaciones para mitigar los riesgos.

4.1.5 Recomendación

En base al análisis y al proyecto planteado, es responsabilidad de las autoridades de la UTIC aplicar y poner en marcha las recomendaciones emitidas de la auditoría informática.

4.2 Informe Detallado.

Posteriormente de Analizar e identificar los riesgos TI más críticos (procesos, prácticas de gestión, actividades y documentación referente) de acuerdo a la Matriz de Riesgos TI y al Plan de Investigación de Campo basados en el marco de referencia COBIT 5, se pudo obtener un conjunto de observaciones y recomendaciones los cuales se indican en el Informe Detallado, el cual fue presentado y analizado con el Sr. Ing. Rubén Arroyo, Director de Tesis.

Construir, Adquirir e Implementar (BAI)

Este dominio cubre los siguientes procesos a evaluar (Matriz de riesgos), Análisis que se realizó para identificar soluciones TI que necesitan ser identificadas, desarrolladas e implementadas, para garantizar el cumplimiento de los objetivos y generar valor al negocio.

Procesos (BAI)

BAI01 Gestionar los programas y Proyectos

BAI02 Gestionar la definición de requisitos

BAI04 Gestionar la Disponibilidad y la Capacidad

BAI06 Gestionar los Cambios

PROCESO: BAI01 Gestionar los programas y Proyectos

PRACTICA DE GESTIÓN:

BAI01.01 Mantener un enfoque estándar para la gestión de programas y proyectos.

Observación:

- La UTIC no sigue una metodología o marco de referencia basado en buenas prácticas para la gestión de programas y proyectos.

Criterio:

“Mantener un enfoque estándar para la gestión de programas y proyectos que posibilite revisiones y tomas de decisión de gobierno y de gestión y actividades de gestión de la entrega, enfocadas en la consecución de valor y de objetivos (requisitos, riesgos, costes, cronograma y calidad) para el negocio de una forma consistente”

Condición:

- No existen requisitos para revisiones de cambio de estado. (No existe documentación de Auditoría)

Causa:

- Falta de metodología y normativas en la gestión de programas y proyectos.
- Falta de requisitos para revisiones de cambio de estado

Efecto:

- Al no tener requisitos para revisiones de cambio de estado, no se puede valorar el status de cumplimiento de las necesidades institucionales.

Recomendación:

- Asentar una Guía estandarizada para la gestión de programas, proyectos y buenas prácticas basadas en procesos definidos, el cual debe ser evaluado periódicamente para fortalecer la gestión de programas y proyectos.

PRACTICA DE GESTIÓN:

BAI01.02 Iniciar un programa.

Observación:

- La UTIC no tiene un plan que valide el cumplimiento de beneficios planificados por cada programa.

Criterio:

“Iniciar un programa para confirmar los beneficios esperados y para obtener la autorización para proceder. Esto incluye los acuerdos sobre el patrocinio del programa, confirmar el mandato del programa a través de la aprobación del caso de negocio conceptual, designar a los consejeros o los miembros del comité del programa, generar el expediente del programa, revisar y actualizar el caso de negocio, desarrollar un plan de realización de beneficios y obtener la aprobación de los patrocinadores para empezar”

Condición:

- La planificación de inicio de programas se ejecuta únicamente cuando existe un presupuesto asignado y aprobado anualmente en función del gasto de cada período. ANEXOS (Evidencia: CATALOGO DE PROYECTOS 2014)

Causa:

- La falta de planificación y políticas de gestión continúa a los beneficios planificados.

Efecto:

- La falta de planificación y políticas de gestión, producen demoras en la ejecución de los programas y no permite el mejoramiento de los servicios y la toma de decisiones.

Recomendación:

- 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.

PRACTICA DE GESTIÓN:

BAI01.03 Gestionar el compromiso de las partes interesadas.

Observación:

- La UTIC no tiene documentación de compromisos de las partes interesadas de programas y proyectos.

Criterio:

"Gestionar el compromiso de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna, que llegue a todos las partes interesadas relevantes. Esto incluye la planificación, identificación y el compromiso de las partes interesadas y la gestión de sus expectativas"

Condición:

- Los compromisos de las partes interesadas no son controlados por indicadores de desempeño, gestión en los procesos y fechas comprometidas. ANEXOS (Evidencia: Cuestionario No.1)

Causa:

- Falta de planificación y procedimientos de gestión de las partes interesadas.
- Falta de conocimiento de los requisitos
- Falta de comunicación y supervisión adecuada (Seguimiento)

Efecto:

- La no aprobación de contratos por parte de la administración y el consejo legal.
- El no cumplimiento de fechas comprometidas para la ejecución de los proyectos.

Recomendación:

- Al Administrador de Contrato: 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.

PRACTICA DE GESTIÓN:

BAI01.04 Desarrollar y mantener el plan de programa.

Observación:

- La UTIC cuenta con un plan para desarrollar y mantener el trabajo a ser efectuado mediante la formalización del alcance que parcialmente satisface los requerimientos del negocio.

Criterio:

"Formular un programa para definir las bases iniciales y posicionarlo para una ejecución exitosa mediante la formalización del alcance del trabajo a ser efectuado e identificando los entregables que satisfarán sus objetivos y la entrega de valor. Mantener y actualizar el plan del programa y el caso de negocio a lo largo del ciclo de vida económico completo del programa, asegurando el alineamiento con los objetivos estratégicos y reflejando el estado actual y los conocimientos obtenidos hasta el momento"

Condición:

- Existe documentación en formato digital pero está incompleta, información que no detalla el plan de programas. ANEXOS (Evidencia: Cuestionario No.1)

Causa:

- Falta de procesos y normatividad en la elaboración del plan de programas.

Efecto:

- Riesgo en la continuidad de plan de programas.

Recomendación:

- 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, así como las reestructuraciones organizacionales necesarias para lograr los resultados que la empresa espera del programa.

PRACTICA DE GESTIÓN:

BAI01.05 Lanzar y ejecutar el programa.

Observación:

- No existe un análisis de Administrar cada programa o proyecto para asegurar que la toma de decisiones y las actividades de entrega están enfocadas en el valor mediante la consecución de los beneficios y las metas del negocio de una manera consistente, considerando el riesgo y alcanzando los requerimientos de las partes interesadas.

Criterio:

“Lanzar y ejecutar el programa para adquirir y dirigir los recursos necesarios para lograr las metas y beneficios definidos en el plan del programa. De acuerdo con los criterios de revisión de lanzamiento o cambio de fase (stage-gate), preparar los cambios de fase, las revisiones de las iteraciones o versiones para informar del progreso del programa y ser capaz de establecer los fundamentos para la financiación de la siguiente etapa después de la revisión del lanzamiento o de cambio de fase (stage-gate)”

Condición:

- No existe documentación, La UTIC INFORMA QUE SE IMPLEMENTARÁ EN LOS PROCESOS QUE SE ESTAN ELABORANDO ALINEADOS A COBIT 5

Causa:

- Normas inexistentes.
- No existe evidencia de un proceso para lanzar y ejecutar un programa.

Efecto:

- No se puede dar seguimiento a los programas y proyectos.

Recomendación:

- Administrador de Contrato: Planificar, dar recursos y asignar las responsabilidades requeridas para los proyectos necesarios para logar los resultados del programa, basados en las revisiones de financiación y las aprobaciones en cada revisión de cambio de fase (stage-gate).

PRACTICA DE GESTIÓN:

BAI01.06 Supervisar, controlar e informar de los resultados del programa

Observación:

- No existe una supervisión y control de los resultados de los programas, así como la verificación de las fechas de implementación y puesta en servicio.

Criterio:

“Supervisar y controlar el rendimiento del programa (entrega de soluciones) y de la organización (valor/resultado) versus el plan durante el ciclo de vida económico completo de la inversión. Informar del rendimiento al comité estratégico del programa y a los patrocinadores”

Condición:

- No existe documentación, La UTIC INFORMA QUE SE IMPLEMENTARÁ EN LOS PROCESOS QUE SE ESTAN ELABORANDO ALINEADOS A COBIT 5

Causa:

- Inadvertencia del problema a generarse.

Efecto:

- Información escasa sobre el status de programas y proyectos.

Recomendación:

- Supervisar y controlar el rendimiento del programa general y de los proyectos dentro del programa, incluyendo la contribución al negocio y a TI de los proyectos, e informar de una manera oportuna, completa y veraz. Los informes pueden incluir cronogramas, financiación, funcionalidad, satisfacción del usuario, controles internos y aceptación de responsabilidades.

PRACTICA DE GESTIÓN:

BAI01.07 Lanzar e iniciar proyectos dentro de un programa.

Observación:

- Se cuenta con una matriz de proyectos la cual no está estructurado

Criterio:

"Definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar entre las partes interesadas un entendimiento común o el alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa general de inversiones de TI. La definición debería estar formalmente aprobada por el patrocinador del programa y del proyecto."

Condición:

- Existe documentación en formato digital pero está incompleta, información que no detalla el alcance de los proyectos. ANEXOS (Evidencia: Cuestionario No.1)

Causa:

- No existe evidencia de un proceso de entendimiento común del alcance del proyecto entre las partes interesadas

Efecto:

- No se puede dar seguimiento a los programas y proyectos.

Recomendación:

- Administrador de Contrato: Crear un entendimiento común del alcance del proyecto entre las partes interesadas, proveer a las partes interesadas de una declaración clara y por escrito que defina la naturaleza, alcance y beneficio de cada proyecto.

PRACTICA DE GESTIÓN:

BAI01.08 Planificar proyectos.

Observación:

- La UTIC posee un formato General, en el cual realiza la planificación de los proyectos, en base a las necesidades institucionales y presupuesto asignado.

Criterio:

“Establecer y mantener un plan de proyecto formal, aprobado e integrado (que cubra los recursos del negocio y de TI), para guiar la ejecución del proyecto y controlarlo durante toda su vida. El alcance de los proyectos debería estar claramente definido y vinculado claramente a la construcción o aumento de la capacidad del negocio”

Condición:

- Existe documentación en formato digital pero está incompleta, información que no detalla la planificación de los proyectos. ANEXOS (Evidencia: FORMATO PROYECTOS PROGRAMACION INVERSIONES ANUAL)

Causa:

- Se cuenta con documentación escasa y desactualizada, lo que ocasiona falencias en la planificación de los proyectos

Efecto:

- Planes de contratación y adquisición que no se ejecuten por temas de falencias en la planificación.

Recomendación:

- Director de la UTIC: Establecer un marco base del proyecto (por ejemplo, coste, cronograma, alcance, calidad) que es debidamente revisado, aprobado e incorporado en el plan de proyectos integrado.

PRACTICA DE GESTIÓN:

BAI01.09Gestionar la calidad de los programas y proyectos.

Observación:

- No existe una gestión a la calidad de los programas y proyectos

Criterio:

“Preparar y ejecutar un plan y procesos y prácticas de gestión de la calidad, alineadas al SGC que describe el enfoque de calidad del programa y el proyecto y cómo será implementado. El plan debería ser formalmente revisado y acordado por todas las partes afectadas y, después, incorporado en los planes integrados del programa y los proyectos“

Condición:

- La gestión a la calidad de los programas y proyectos, no se da seguimiento ya que no existe un proceso para ejecutar está gestión. La UTIC INFORMA QUE SE IMPLEMENTARÁ EN LOS PROCESOS QUE SE ESTAN ELABORANDO ALINEADOS A COBIT 5

Causa:

- Normas inadecuadas, ineficientes.
- Falta de políticas para la gestión.

Efecto:

- Retraso en la ejecución, calidad de los programas y proyectos.
- Inefectividad en el trabajo (No se ejecuta conforme a la planificación)

Recomendación:

- Director de la UTIC: Realizar aseguramiento de la calidad y actividades de control de acuerdo con el plan de gestión de la calidad y el SGC.

PRACTICA DE GESTIÓN:

BAI01.10 Gestionar el riesgo de los programas y proyectos.

Observación:

- La UTIC posee un formato General, en la cual elabora la matriz de riesgos de cada proyecto, análisis que no es apropiado para los procesos de negocio.

Criterio:

“Eliminar o minimizar los riesgos específicos asociados con los programas y proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta, supervisión y control de las áreas o eventos que tienen el potencial de causar cambios no deseados. Los riesgos enfrentados por la administración del programa y los proyectos deberían ser establecidos y registrados en un único punto”

Condición:

- Existe documentación en formato digital pero está incompleta, información que no detalla los riesgos por proyecto. ANEXOS (Evidencia: FORMATO PROYECTOS)

Causa:

- Falta de normativas
- No se emplea un análisis solido de riesgos referentes a los procesos del negocio.

Efecto:

- No se identifica adecuadamente riesgos asociados con los procesos del negocio.

Recomendación:

- Directo de la UTIC: Realizar un análisis de riesgo del proyecto para identificar y cuantificar el riesgo de manera continua durante el proyecto.

- Gestionar y comunicar el riesgo adecuadamente dentro de la estructura de gobierno del proyecto.

PRACTICA DE GESTIÓN:

BAI01.11 Supervisar y controlar proyectos.

Observación:

La UTIC asigna un responsable por proyecto para la ejecución del programa.

Criterio:

“Medir el desempeño del proyecto versus los criterios clave de rendimiento del proyecto, tales como la planificación, la calidad, el coste y los riesgos. Evaluar el impacto de las desviaciones en el proyecto y el programa general e informar los resultados a las partes interesadas clave”

Condición:

Existe documentación en formato digital pero está incompleta, información que no detalla el alcance del responsable por proyecto. ANEXOS (Evidencia: FORMATO PROYECTOS).

Causa:

- Falta de procesos y normatividad en el proceso de supervisar y controlar proyectos.

Efecto:

- Impacto en la planificación de los proyectos y bajo desempeño de los requerimientos de negocio.

Recomendación:

- Director de la UTIC: Recomendar y supervisar las acciones correctivas, cuando sean requeridas, en línea con el marco de gobierno de programas y proyectos.

PRACTICA DE GESTIÓN:

BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto.

Observación:

- La UTIC asigna un responsable por proyecto para gestionar los recursos y paquetes de trabajo del proyecto.

Criterio:

- "Gestionar los paquetes de trabajo mediante requerimientos formales de autorización y aceptación de los paquetes de trabajo, y asignando y coordinado los recursos de negocio y de TI adecuados".

Condición:

- Existe documentación en formato digital pero está incompleta, información que no detalla el responsable por proyecto. ANEXOS (Evidencia: FORMATO PROYECTOS).

Causa:

- Falta de planificación para gestionar los recursos y los paquetes de trabajo.

Efecto:

- No se analiza el grado de cumplimiento de la gestión de recursos y paquetes de trabajo de los proyectos.
- Control inadecuado de los recursos y paquetes de trabajo.

Recomendación:

- Planificar y supervisar las acciones correctivas, cuando sean requeridas, en línea con el marco de gobierno de programas y proyectos.

PRACTICA DE GESTIÓN:

BAI01.13 Cerrar un proyecto o iteración.

Observación:

- Todo proyecto se cierra luego de la elaboración de la acta entrega recepción.

Criterio:

“Solicitar a las partes interesadas del proyecto, al final de cada proyecto, versión o iteración, que evalúen si el proyecto, la versión o la iteración entregaron los resultados y valor planeados. Identificar y comunicar cualquier actividad pendiente necesaria para lograr los resultados del proyecto y los beneficios del programa planeados, identificar y documentar las lecciones aprendidas para futuros proyectos, versiones, iteraciones y programas”.

Condición:

- Existe documentación en formato digital pero está incompleta, información que no detalla el cierre de los proyectos del año 2014 (Evidencia: CATALOGO DE PROYECTOS 2014).

Causa:

- Falta de procesos de cierre de proyectos.

Efecto:

- Riesgo en la regularización de pagos de los proyectos.

Recomendación:

- Director de la UTIC: Planificar y ejecutar revisiones post-implementación para determinar si los proyectos entregaron los beneficios esperados y para mejorar la metodología de gestión de proyecto y el proceso de desarrollo de sistemas.

PRACTICA DE GESTIÓN:

BAI01.14 Cerrar un programa.

Observación:

- No existe un plan para cerrar los programas y proyectos.

Criterio:

“Eliminar el programa del portafolio de inversiones activas cuando haya acuerdo de que el valor deseado ha sido logrado o cuando esté claro que no será logrado con los criterios de valor establecidos para el programa”.

Condición:

- No existe documentación, ni plan para cerrar los programas y proyectos.

Causa:

- Falta de planificación.
- Falta de normatividad relativa al tema.

Efecto:

- Retardos en la regularización de pagos a proveedores.
- Retardos en la implementación de proyectos ejecutados por fases.

Recomendación:

- Director de la UTIC: Llevar el programa a un cierre ordenado, incluyendo una aprobación formal, desmantelamiento de la organización del programa y la función de apoyo, validación de los entregables y comunicación de la retirada.

PROCESO: BAI02 Gestionar la definición de requisitos

PRACTICA DE GESTIÓN:

BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio.

Observación:

- El proceso de definición y mantenimiento de requerimientos técnicos y funcionales de negocio no se efectúa para todos los proyectos.

Criterio:

“Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información de negocio, funcionales, técnicos y de control que cubra el alcance/entendimiento de todas las iniciativas necesarias para alcanzar los resultados esperados de la solución de negocio de TI propuesta.”

Condición:

- No existe documentación de análisis costo beneficio de los proyectos.

- No existe documentación de un proceso, plan, metodología y estándares para soluciones automatizadas.

Causa:

- Falta de normatividad, en base a políticas.

Efecto:

- Al no realizar un análisis de costo beneficio no se puede establecer las ventajas de ejecutar los proyectos.

Recomendación:

- Elaborar políticas y Normativas para 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.

PRACTICA DE GESTIÓN:

BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas.

Observación:

- No existe evidencia de estudios de viabilidad para proponer soluciones alternativas.

Criterio:

- “Realizar un estudio de viabilidad de las potenciales soluciones alternativas, evaluando su viabilidad y seleccionando la opción preferida. Si se considera, implementar la opción seleccionada como un piloto para determinar posibles mejoras”

Condición:

- No existe documentación de soluciones alternativas con todas las partes interesadas, incluyendo costes y riesgos.

Causa:

- Falta de un análisis para identificar las acciones requeridas para la adquisición o desarrollo de soluciones.

Efecto:

- La falta de soluciones alternativas, afecta principalmente a los requerimientos de efectividad y disponibilidad de los servicios del negocio.

Recomendación:

- Administrador de contrato: Elaborar 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.

PRACTICA DE GESTIÓN:

BAI02.03 Gestionar los riesgos de los requerimientos.

Observación:

- No existe evidencia de gestión de riesgos de requerimientos de los proyectos.

Criterio:

“Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa y solución propuesta”

Condición:

- No existe documentación de modos de controlar, evitar o mitigar los riesgos de los requerimientos en orden de prioridad.

Causa:

- Falta de planificar, analizar y priorizar los riesgos de los requerimientos conforme probabilidad e impacto.

Efecto:

- Si no se identifican amenazas y vulnerabilidades, los proyectos no se ejecutan de forma óptima.

Recomendación:

- Director de tesis: Involucrar a las partes interesadas para crear una lista potencial de requerimientos técnicos, funcionales, de calidad y riesgos relativos al procesamiento de la información

PRACTICA DE GESTIÓN:

BAI02.04 Obtener la aprobación de los requerimientos y soluciones

Observación:

- No existe evidencia del alcance de las soluciones.

Criterio:

"Coordinar la realimentación de las partes interesadas afectadas y, en las fases clave predeterminadas, obtener la aprobación y la firma del patrocinador o propietario del producto y cierre de los requerimientos técnicos y funcionales, de los estudios de viabilidad, de los análisis de riesgos y de las soluciones recomendadas".

Condición:

- No existe documentación de una retroalimentación de las partes interesadas en las fases clave predeterminadas para obtener la aprobación y la firma del patrocinador o propietario del producto y cierre de los requerimientos técnicos y funcionales.

Causa:

- No existe una planificación sobre cada fase del proyecto.

Efecto:

- No satisfacer a las partes interesadas con la solución implementada.

Recomendación:

- Administrador de contrato: Elaborar un plan de trabajo en base a los requerimientos y soluciones a ejecutar, para luego validar el cumplimiento de las necesidades de las partes interesadas.

PROCESO: BAI04 Gestionar la Disponibilidad y la Capacidad

PRACTICA DE GESTIÓN:

BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.

Observación:

- No existe evidencia de evaluaciones de disponibilidad, rendimiento y capacidad actual.

Criterio:

- “Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados”.

Condición:

- No existe documentación de evaluaciones de disponibilidad, rendimiento y capacidad actual.
- No existen métodos de seguimiento para gestionar la disponibilidad y capacidad.

Causa:

- Falta de políticas y normativas para evaluar la disponibilidad, rendimiento y capacidad actual

Efecto:

- Deficiente gestión para mantener la disponibilidad del servicio, la gestión eficiente de recursos y la optimización del rendimiento.

Recomendación:

- Administrador de contrato: Evaluar periódicamente los niveles reales de rendimiento a todos los niveles de procesamiento (la demanda del negocio, capacidad de servicio y capacidad de los recursos) mediante la comparación con las tendencias y los ANSs, teniendo en cuenta los cambios en el entorno.

PRACTICA DE GESTIÓN:

BAI04.02 Evaluar el impacto en el negocio.

Observación:

- No existe evidencia de informes de servicios críticos del negocio.

Criterio:

"Identifica los servicios importantes para la empresa, mapear los servicios y recursos con los procesos de negocio e identificar las dependencias del negocio. Asegurar que el impacto de la indisponibilidad de recursos está acordado y aceptado por el cliente. Asegurar que, para las funciones vitales del negocio, los requisitos de disponibilidad definidos en el ANS pueden ser satisfechos"

Condición:

- No existe documentación de un análisis de impacto de negocio.

Causa:

- Falta de políticas y procedimientos para evaluar el impacto del negocio.

Efecto:

- No garantizar la disponibilidad de los servicios que provee la institución.

Recomendación:

- Administrador de contrato: Identificar los servicios críticos para los procesos de gestión de la disponibilidad y la capacidad, para luego priorizar y ejecutar planes de contingencia ante posibles fallas.

PRACTICA DE GESTIÓN:

BAI04.03 Planificar requisitos de servicio nuevos o modificados.

Observación:

- No existe evidencia de planificación de cambios y nuevos servicios.

Criterio:

“Planificar y priorizar las implicaciones en la disponibilidad, el rendimiento y la capacidad de cambios en las necesidades del negocio y en los requerimientos de servicio”.

Causa:

- Falta de políticas y normativas para planificar y aprobar cambios y nuevos servicios.

Efecto:

- Desconocimiento de las partes interesadas de cambios y nuevos servicios a implementar.

Recomendación:

- Administrador de contrato: Identificar las implicaciones en la disponibilidad y la capacidad de cambios en las necesidades del negocio y oportunidades de mejora. Utilizar técnicas de modelado para validar los planes de disponibilidad, rendimiento y capacidad.

PRACTICA DE GESTIÓN:

BAI04.04 Supervisar y revisar la disponibilidad y la capacidad.

Observación:

- No existe evidencia de un proceso de recolección de datos para proporcionar información de seguimiento e informes de la carga de trabajo de disponibilidad, rendimiento y capacidad de todos los recursos relacionados con la información.

Criterio:

- “Supervisar, medir, analizar, informar y revisar la disponibilidad, el rendimiento y la capacidad. Identificar desviaciones respecto a las líneas de referencia establecidas. Revisar informes de análisis de tendencias identificando cualquier cuestión y variación significativa, iniciando acciones donde sea necesario y asegurando que se realiza el seguimiento de todas las cuestiones pendientes”.

Condición:

- No existe documentación de un procedimiento para validar la disponibilidad y la capacidad de los servicios.

Causa:

- Falta de políticas y procedimientos para supervisar y revisar la disponibilidad y la capacidad.

Efecto:

- Riesgo de no disponibilidad y escalabilidad del servicio que se provee.

Recomendación:

- Administrador de contrato: Proporcionar información periódica de los resultados en una forma apropiada a director de la UTIC, autoridad que en base a la información facilitada tomará decisiones para la mejora de los procesos.

PROCESO: BAI06 Gestionar los Cambios

PRACTICA DE GESTIÓN:

BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio.

Observación:

- No existe evidencia de un proceso para gestionar los cambios

Criterio:

- “Evaluar todas las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI, y analizar si el cambio afectará negativamente al entorno operativo e introducirá un riesgo inaceptable. Asegurar que los cambios son registrados, priorizados, categorizados, analizados, autorizados, planificados y programados”

Condición:

- No existe documentación de un registro de los cambios realizados y su justificación.

Causa:

- Falta de políticas y normativas relacionada al proceso.

Efecto:

- No disponer de documentación necesaria para validar las mejoras de los cambios realizados y posibles indicadores que ayuden a la mejora continua.

Recomendación:

- Administrador de contrato: Elaborar políticas y procedimientos para priorizar todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio, recursos necesarios, así como las razones contractuales, legales o de regulación que motivan el cambio.

PRACTICA DE GESTIÓN:

BAI06.02 Gestionar cambios de emergencia.

Observación:

- No existe evidencia de un comité de cambios para autorizar su ejecución.
- No existen políticas y procedimientos para la atención y gestión de cambios de emergencia.

Criterio:

“Gestionar cuidadosamente los cambios de emergencia para minimizar futuras incidencias y asegurar que el cambio está controlado y se realiza de forma

segura. Verificar que los cambios de emergencia son evaluados debidamente y autorizados una vez hecho el cambio”

Condición:

- No existe documentación de un registro de los cambios de emergencia y comités de cambios.

Causa:

- No existe procedimientos ni controles para manejo de cambios de emergencia y procesos (Rollback) para poder deshacer los cambios de manera oportuna si existiese algún problema con el cambio ejecutado.

Efecto:

- Control inadecuado de todos los cambios considerados como urgentes, cambios que deben ser analizados y priorizados para garantizar la disponibilidad de los servicios.

Recomendación:

- Administrador de contrato: Elaborar políticas y procedimientos, para tener un control de todos los cambios realizados y así garantizar la disponibilidad de los servicios de la institución.

PRACTICA DE GESTIÓN:

BAI06.03 Hacer seguimiento e informar de cambios de estado.

Observación:

- No existe evidencia de un proceso o políticas de seguimiento y status a detalle de los cambios realizados.

Criterio:

“Mantener un sistema de seguimiento e informe que documente los cambios rechazados, comunique el estado de cambios aprobados y en proceso y de cambios completados. Asegurar que los cambios aprobados son implementados como esté previsto”.

Condición:

- No existe documentación sobre procesos de cambio de estado.

Causa:

- No existen políticas y procedimientos definidos para el seguimiento de cambios de estado.

Efecto:

- Al no tener un proceso de seguimiento apropiado, no se puede evaluar si las acciones que se tomaron fueron óptimas y adecuadas en un periodo apropiado para no afectar el funcionamiento de los sistemas.

Recomendación:

- Administrador de contrato: Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado, asegurando que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre.

PRACTICA DE GESTIÓN:

BAI06.04 Cerrar y documentar los cambios.

Observación:

- No existe evidencia de procesos de cierre y documentos de cambios realizados.

Criterio:

“Siempre que el cambio haya sido implementado, actualizar, de manera consecuente, la documentación de la solución y del usuario, así como los procedimientos a los que afecta el cambio”.

Condición:

- No existe evidencia de políticas y procesos de cierre y cambios.

Causa:

- No se tiene definido ningún procedimiento de cierre y cambios realizados.
- No existen controles al momento de realizar los cambios.

Efecto:

- Debido a la falta de procedimientos, no se tiene un catálogo de conocimiento sobre cambios realizados.

Recomendación:

- Administrador de contrato: Elaborar políticas y procedimientos, los cuales abarquen con información detallada (procesos, sistemas, parámetros, versiones, etcétera) de todos los cierres y cambios ejecutados. Información necesaria para identificar el status de cada solicitud de cambio.

4.3 Evidencias.

La información recopilada es documentación facilitada por la Unidad de Tecnología de la Información y Comunicación (UTIC) y encuestas elaboradas por el equipo de auditoría. ANEXOS.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5. 1 Conclusiones y Recomendaciones

Al finalizar el proyecto de tesis con asunto evaluación técnica informática de la ESPE sede principal, se cumplió con los objetivos propuestos en el siguiente proyecto, motivo por el cual se exponen las conclusiones y recomendaciones.

5.2 Conclusiones

- Para el desarrollo del proyecto de tesis es de principal importancia contar con una guía de un marco de referencia. Modelo COBIT5 que se seleccionó, el cual a través de su dominio construir, adquirir e implementar, ofrece una serie de prácticas de gestión que permiten evaluar eficientemente el ambiente de control de una entidad, garantizando que TI este alineado con el negocio y que los riesgos de TI se administren apropiadamente.
- COBIT 5 facilita al auditor a tener una visión más objetiva y de un nivel más estratégico para planear, organizar, dirigir y controlar una auditoría a los procesos dentro de una organización. Así como también de guía para la mejora de los procesos internos de la institución.
- En el proceso de auditoría que se realizó en la UTIC, se cumplió con todas las expectativas del proyecto, y se observó que al ser una institución pública, carece de políticas y procedimientos en los procesos de Adquisición e implementación; existiendo el riesgo de que la calidad de la administración y servicio de TI sea deficiente y no se considere una adecuada planificación por parte de la Unidad de Tecnología de la Información y Comunicaciones.
- Al alinear la normativa respecto a TI y las prácticas de gestión propuestas por COBIT se logró identificar y valorar los riesgos dentro de la UTIC, para luego tomar las acciones pertinentes y mitigar la materialización de los riesgos identificados.

- La auditoría informática propone mejora a los controles existentes en la UTIC, al mejorar los controles que tienen vulnerabilidades se logra mitigar los riesgos. Controles que deben estar en conocimiento de las partes interesadas.
- En las entidades públicas existen retrasos en facilitar información para elaborar proyectos de auditoría informática, generadas por las tareas diarias que realizan; circunstancias que alteran el cronograma de trabajo del grupo de auditoría.

5.3 Recomendaciones

- Elaborar una planificación para que la Unidad de Tecnologías de la Información y Comunicaciones (UTIC), analice y ejecute las observaciones y recomendaciones del presente proyecto de Auditoría.
- La UTIC debe dar apertura a este tipo de evaluación de sus funciones, colaborando con la documentación y evidencias necesarias manteniendo registros documentados de las actividades que realizan.
- Se recomienda que para un mejor desempeño de la UTIC, se realicen auditorías anuales en sus áreas, revisando especialmente las guías de gestión de TI y las necesidades de la institución.
- Se recomienda coordinar con la unidad que está dentro del alcance de la auditoría, para centralizar esfuerzos y llegar a cumplir con los objetivos planteados.
- Se recomienda la implementación del marco de referencia COBIT 5 en la UTIC para la administración de los recursos de tecnología. Estándar que debe ser oficialmente la guía para la mejora de los procesos internos de la institución.
- Se sugiere que se tome acciones en los procesos de Adquisición e implementación con documentación respectiva, efectuando estrategias que

permitan tener un mayor control en los proyectos, ayudando a los intereses y requerimientos de la institución. Además se debe definir cada una de las funciones, actividades y responsabilidades específicas adecuadamente para cada individuo involucrado en la UTIC.

- La UTIC como directivos que son, deben capacitarse y abrirse acerca de proyectos de este tipo, para que sean entes colaboradores más no de disturbio y freno a la ejecución de los mismos.
- Proponer el pago de horas extras al personal de la ESPE que participa en los proyectos de auditoría, tiempo adicional que es necesario para facilitar toda la información y documentación de los procesos auditados.

BIBLIOGRAFÍA

- Londoño, L. (2014). GUÍA PARA CONSTRUIR ESTADOS DEL ARTE. 2015, Sitio web: http://www.colombiaaprende.edu.co/html/investigadores/1609/articles-322806_recurso_1.pdf
- Muñoz, I., & Ulloa, G. (2011). Gobierno de TI. Revista S&T, 9(17), 23-53. Cali: Universidad Icesi.
- Universidad EAFIT. (2007). MODELO PARA AUDITORIA Y CONTROL DE SISTEMAS DE INFORMACIÓN. Sitio web: http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/COBIT%20audit%20y%20ctrol%20sists%20inf.pdf
- Prandini, P.,& Zsuster, R . (2012). COBIT. 2015, de SEGURINFO Sitio web: http://www.ccpa.or.cr/file/isaca/dia1/5-evolucion-de-cobit-4-1-a-5-alvaro-jaikel.pdf
- Rojas, I. (2013). COBIT., de Monografias.com Sitio web: http://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt
- Villad, R. (2015). Administración de Riesgos., de Unisys Sitio web: http://www.acis.org.co/memorias/JornadasSeguridad/IIJNSI/administracion.ppt
- Erb, M. Gestión de Riesgo en la Seguridad Informática, de Creative Commons Atribución Sitio web: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/
- López, L. (2012). Administración de Riesgo Empresarial. 123, de 123 Sitio web: http://catarina.udlap.mx/u_dl_a/tales/documentos/lat/salgado_a_a/capitulo2.pdf
- Hamilton, A. (1982). Clave del mejoramiento financiero y operativo de la Auditoría Interna: EEUU.

- Quiroc, M.C. (2003). Administración del riesgo y Auditoría Interna. Universidad de Costa Rica. Contraloría Universitaria. Sitio web: http://ucu.ucr.ac.cr/boletin1-2003.artículo9.htm
- Rosés, F. (2000). El mapa de riesgos permite ver las amenazas que tiene la empresa. Sitio web: http://wwwdiariomedico.com/gestion/ges.220300.com.
- Noguera, F. (2013). Auditoría Interna en la Gestión de Riesgos. de Deloitte Sitio web: http://www.ccpa.or.cr/file/mayo_2013/charlas/15-6-el-rol-del-auditor-interno-en-la-gestion-de-riesgo.ppt.
- Hernandez, E. (2007). Administración de Riesgos en Auditoría Interna., de Monografías.com Sitio web: http://www.monografias.com/trabajos47/riesgos-auditoria-interna/riesgos-auditoria-interna.shtml
- Alvarez, D. (2005). Seguridad Informática., de Universidad Iberoamericana Sitio web: http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf
- Alvarez, L.. (2005). SEGURIDAD EN INFORM ÁTICA - AUDITORÍA DE SISTEMAS., Sitio web: http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf
- Nara, J. (2011). APUNTES DE AUDITORÍA INFORMÁTICA ., Sitio web: http://www.escet.urjc.es/~ai/T1Apuntes.pdfhttp://repositorio.espe.edu.ec/bitstream/21000/5239/2/T-ESPE-033151-A.pdf
- Jo, J.(2008). COBIT-AI., Sitio web: http://cobit-ai.blogspot.com/2008/12/adquisicin-hardware.htmles/~ai/T1Apuntes.pdf
- Lopez, R. (2012). Cobit: Dominio 2: Adquisición e Implementación. , de slideshare Sitio web: http://es.slideshare.net/Metalrider666/cobit-dominio-2-adquisicin-e-implementacin
- Santacruz, J. (2014). COBIT ADQUISICIÓN E IMPLANTACIÓN. , de ACADEMIA.EDU Sitio web: http://www.academia.edu/9160053/ADQUISICION_E_IMPLANTACION

- Aucancela, J. (2014). AUDITORIA DE RIESGOS INFORMATICOS A PYMES UTILIZAND O ., de CAVES SA EMA Sitio web: http://repositorio.espe.edu.ec/bitstream/21000/6094/1/AC-MGS-ESPE-034400.pdf
- Rojas, I. (2013). Análisis y Gestión Riesgo., de Monografias.com Sitio web: http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml#ixzz3TGI46cnV
- Julio, A. (2012). Adquisicion e implementacion cobit., de slideshare Sitio web: http://es.slideshare.net/julioandres55/adquisicion-e-implementacion-cobits.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml#ixzz3TGI46cnV

ANEXOS