UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERIA

MAESTRÍA EN GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN

TESIS

DIAGNÓSTICO Y PLAN DE ACCION PARA LA IMPLEMENTACION DEL MARCO DE NEGOCIO PARA EL GOBIERNO Y GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN (COBIT5.0) APLICADO A LA UNIVERSIDAD TÉCNICA DE MACHALA.

PREVIO A LA OBTENCIÓN DEL GRADO DE MAGISTER EN GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR: Ing. Wilmer Braulio Rivas Asanza.
CI: 0702580192
DIRECTOR: Ing. Jorge Luis Bermeo Conto. Msc.
CI: 0103900387

CUENCA-ECUADOR

2017

Resumen

La tecnología debe ser un auténtico aliado estratégico de las empresas, más allá de un simple soporte, proporcionando el valor y la eficiencia que exigen tanto el negocio como los usuarios. Así, en este escenario, se introduce el concepto de Gobierno de TI como el responsable de integrar e institucionalizar las buenas prácticas de Gestión de TI para garantizar que las TI en la empresa soportan los objetivos del negocio y se aprovecha al máximo su información, se maximizan los beneficios, se capitalizan las oportunidades y se ganan ventajas competitivas. En este sentido la propuesta de este trabajo es incorporar el marco de trabajo COBIT5.0 de Gobierno y Gestión como herramienta para realizar el diagnóstico situacional de la Universidad Técnica de Machala respecto de los procesos que plantea COBIT5.0; el diagnóstico se lo realizará usando el modelo de capacidades y la información de los procesos catalizadores a través de una auditoria de cumplimiento obteniendo el nivel de capacidad de los procesos de la Institución. Luego establecer con la alta gerencia que procesos son prioritarios mediante el modelo de cascada de COBIT5.0. , de los procesos que resultaren más prioritarios establecer una hoja de ruta o plan de acción de las actividades que deben desarrollarse para la implementación de los mismos y finalmente se propone desarrollar productos entregables como plantillas, procedimientos, controles, manual que permita alcanzar el nivel de capacidad deseado en esos procesos.

Palabras claves: Gobierno de TI, gestión de TI, Cobit5.0

Abstract

The technology must be a true strategic ally of the companies, beyond a simple support, providing the value and efficiency that both the business and the users demand. Thus, in this scenario, the concept of IT Governance is introduced as responsible for integrating and institutionalizing good IT Management practices to ensure that IT in the company supports the business objectives and makes the most of its information. Maximize profits, capitalize opportunities and gain competitive advantages. In this sense, the proposal of this work is to incorporate the COBIT5.0 framework of Government and Management as a tool to perform the situational diagnosis of the Technical University of Machala regarding the processes proposed by COBIT5.0; the diagnosis will be made using the capabilities model and the information of the catalytic processes through a compliance audit, obtaining the capacity level of the Institution's processes. Then establish with senior management which processes are priority through the cascade model of COBIT5.0. , of the processes that are more priority to establish a road map or action plan of the activities that must be developed for the implementation of the same and finally it is proposed to develop deliverables such as templates, procedures, controls, manual that allows to reach the level of desired capacity in those processes.

keywords: IT governance, IT management, Cobit5.0.

Tabla de contenido

Lista de tablas

Lista de figuras

Cláusula de licencia y autorización para publicación en el Repositorio Institucional

WILMER BRAULIO RIVAS ASANZA en calidad de autor/a y titular de los derechos morales y patrimoniales del trabajo de titulación "DIAGNÓSTICO Y PLAN DE ACCION PARA LA IMPLEMENTACION DEL MARCO DE NEGOCIO PARA EL GOBIERNO Y GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN (COBIT5.0) APLICADO A LA UNIVERSIDAD TÉCNICA DE MACHALA", de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN reconozco a favor de la Universidad de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos.

Asimismo, autorizo a la Universidad de Cuenca para que realice la publicación de este trabajo de titulación en el repositorio institucional, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Cuenca, 10 de noviembre 2017

WILMER BRAULIO RIVAS ASANZA

C.I: 0702580192

Cláusula de Propiedad Intelectual

WILMER BRAULIO RIVAS ASANZA, autor/a del trabajo de titulación "DIAGNÓSTICO Y PLAN DE ACCION PARA LA IMPLEMENTACION DEL MARCO DE NEGOCIO PARA EL GOBIERNO Y GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN (COBIT5.0) APLICADO A LA UNIVERSIDAD TÉCNICA DE MACHALA", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor/a.

Cuenca, 10 de Noviembre 2017

WILMER BRAULIO RIVAS ASANZA

C.I: 0702580192

Dedicatoria

A Dios por permitir la oportunidad de cumplir una meta más en mi vida; a mis padres por su apoyo incondicional; a mi familia, esposa e hijos que con su esfuerzo y sacrificio han aportado con esta consecución.

Agradecimiento

Al personal de la Universidad Técnica de Machala por su colaboración; de manera especial agradezco a mi tutor Jorge Bermeo, quien con su dirección permitió culminar con éxito el trabajo. También agradezco por su colaboración al Dr. Javier Zalamea y al Dr. Diego Ponce.

CAPÍTULO I

1. INTRODUCCIÓN

1.1 MOTIVACIÓN DEL TRABAJO

En la actualidad existen multitud de factores de riesgo de continuidad del negocio como, por ejemplo, la desaceleración en los mercados asiáticos, los bajos precios del petróleo o las tensiones geopolíticas (Internacional, 2016). El Fondo Monetario Internacional, preocupado por este contexto, advierte de hecho de los significativos riesgos que corren las principales economías de mercado y de la posible disminución del crecimiento económico mundial para los próximos años. Por otra parte, el entorno competitivo es cada vez más incierto y complejo, lo que conlleva una mayor dificultad para las empresas a la hora de conseguir una ventaja competitiva en el tiempo.

Este entorno económico genera, por contra, un clima propicio para que las organizaciones piensen en alternativas de solución que ayuden a mantener los beneficios. En estas circunstancias se convierte, en una motivación el presente trabajo, ya que tanto el Gobierno de Tecnologías de la Información (en adelante, TI) como la Gestión de TI son factores importantísimos para que las organizaciones alcancen la madurez necesaria y puedan desarrollarse en el tiempo mediante una administración que permita generar valor, alineación estratégica y gestión de riesgos.

Todas las organizaciones deben tener un sistema mediante el cual sean dirigidas y controladas. Esto es lo que fundamenta el concepto de Gobierno Corporativo, el cual establece un conjunto de responsabilidades y prácticas ejecutadas por la junta directiva con los objetivos de proveer dirección estratégica (ECONOMICO, 2011). De esta manera, para dar cumplimiento a las estrategias y objetivos de la empresa se presenta el Gobierno de TI como parte integral del Gobierno Corporativo y consiste en el liderazgo, estructuras organizativas y procesos que aseguran el soporte de TI a la organización para dar cumplimiento a las estrategias y objetivos de la empresa (Haris Hamidovic, 2011) (Llorens, 2011).

Para implantar un Gobierno de TI efectivo y eficaz en una organización es lógicamente necesario basarse en un marco de control que muestre el "QUÉ" se debe hacer (i. e., un marco de Gobierno de TI).

Los marcos de trabajo son, en términos generales, un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular, que sirve como referencia para enfrentar y resolver nuevos problemas de índole similar (Mohamad & Toomey, 2016). En este sentido, existen múltiples aproximaciones orientadas hacia el Gobierno de TI (e.g., Cobit5.0:2012, ISO38500, Weill/Ross, Calder&Moir, Forrester). No obstante, para el objeto que aquí ocupa, sólo se considera uno de los más relevantes, significativo y característico: COBIT5.0:2012 (Megias, 2009).

COBIT 5.0:2012 (Control OBjectives for Information and related Technology) es un "marco de trabajo para el Gobierno y la Gestión de TI, organizado para garantizar que el uso de los recursos de TI está efectivamente alineado con las estrategias de negocio de la organización" (Neto & Neto, 2013).

Como muestra de la importancia que supone el Gobierno de TI, se recogen a continuación algunos datos representativos de su evolución e interés en el tema:

- El Instituto de Gobierno de TI (ITGI por sus siglas en inglés), entrevisto a 749 ejecutivos del nivel CEO/CIO en 23 países, la cual fue conducida por el mes de Mayo de 2008, destaca que el porcentaje de organizaciones que están en el proceso de implementar o ya han implementado prácticas de gobierno de TI en las diferentes regiones son: Latinoamérica 27%, Asia 44%, Europa 50%, Norteamérica 50% (Meaddows, 2008).
- La consultora IDC Latinoamérica, presentados en el "CXO Barometer", en mayo de 2014 (America, 2014), menciona que debido a la gran dependencia de los procesos del negocio con la tecnología, tanto los líderes de TI como del negocio se encuentran constantemente buscando

prácticas de gobierno, que los ayuden a alinear las tecnologías de la información con las estrategias empresariales. Por lo tanto, comprender hoy la problemática en torno a la alineación es un punto de partida para que la organización obtenga valor mediante las TI. Es precisamente el concepto de Gobierno de TI el que cataliza y une todos los esfuerzos por integrar políticas, procesos, prácticas y estructuras, orientadas a ofrecer un entorno articulado en la gestión estratégica de TI, dentro de una organización. En la medida en que mayores objetivos estratégicos se soporten bajo las TI, mayor cuidado y atención debe prestarse a su gestión efectiva. Sin embargo, a pesar de estar ampliamente comprendido que el negocio y la estrategia TI deben estar alineados, las naturalezas de estas alineaciones están hoy inadecuadamente establecidas, en la mayoría de nuestras organizaciones.

- Según el Reporte de Estado Global 2011-2012 (Global Status Report) desarrollado por el IT Governance Institute (GERENCIA, 2013), que incluyó respuestas de más de 800 profesionales en 21 países, un 95% considera que el Gobierno de TI es importante o muy importante para que las empresas obtengan valor de sus Tecnologías de Información.
- También, la encuesta realizada a miembros latinoamericanos de ISACA en Chile en el año 2008 determino que en temas de TI el orden de importancia el principal tema es la innovación del negocio (18,1%). Lo sigue Gobierno de TI con un 18% y en tercer lugar está el tema de auditorías en Tecnología de la Información con un 16.9% (ITGI, 2008).

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL.

Definir un plan de acción de las actividades que deben desarrollarse para la implementación de procesos definidos como prioritarios con la alta gerencia luego del análisis de resultados de un diagnóstico de situación inicial basado en COBIT 5.0 para la Universidad Técnica de Machala.

1.2.2 OBJETIVOS ESPECÍFICOS

- Elaborar el estado de arte respecto a los marcos de gobierno y gestión de TI.
- Diagnosticar la situación actual de la Universidad Técnica de Machala respecto de los procesos que plantea COBIT5.0; el diagnostico se lo realizará usando el modelo de capacidad y la información de los procesos catalizadores de COBIT5.0 a través de una auditoria de cumplimiento, obteniendo como resultado el nivel de capacidad de la Institución en los procesos de COBIT5.0.
- Establecer con la alta gerencia que procesos son prioritarios usando el modelo en cascada que propone COBIT5.0
- Establecer una hoja de ruta o plan de acción de las actividades que deben desarrollarse para la implementación de los procesos prioritarios.
- Desarrollar productos entregables que permita alcanzar el nivel de madurez deseado en esos procesos.

1.3 ESTRUCTURA DE LA MEMORIA

- Capítulo I. Introducción.

  El primer capítulo explica el contexto del tema de la tesis de maestría; ¿por qué? existen factores de riesgo que generan un clima propicio para que las organizaciones busquen alternativas para crear valor; así también se referencia cierta definición relacionado con el área de la gobernanza corporativa, gobierno de TI; así como destacar la importancia a través de datos de varias encuestas obtenidas por varios autores, los objetivos de trabajo de la tesis y la estructura de la organización de la tesis.

- Capítulo II. Estado de la cuestión.

  En el capítulo denominado estado de la cuestión o el estado del arte del trabajo, se realiza la revisión de la literatura de los diferentes conceptos relacionados con la tesis, y para ello se profundiza en cuatro aspectos claves, el primero, respecto a literatura en relación al Gobierno de TI; el segundo, respecto a los principales marcos, estándares, guías, etc., más

relevantes en la actualidad para el Gobierno de TI; el tercero, respecto a la literatura en relación a la Gestión de Tecnologías; y finalmente, en relación a los principales marcos, estándares, guías, etc., más relevantes en la actualidad para el Gestión de TI.

- Capítulo III. Diagnóstico

  Este capítulo presenta dos tipos de información, la primera muestra información proporcionada por la UTMACH que permite conocer el entorno de la institución como infraestructura, nivel de organización, análisis FODA y la segunda establece un diagnóstico, se establece el nivel de capacidad de los procesos que propone el marco de trabajo COBIT 5.0.

- Capítulo IV. Procesos prioritarios.

  En este capítulo, se establece los procesos prioritarios mediante el uso de cascada de metas de Cobit5.0 (ISACA, Modelo de Cascada de metas , 2012), cuyo metodología se basa en establecer las preocupaciones de las partes interesadas (las partes interesadas serán definidas de acuerdo a las políticas y controles de cada empresa), estas relacionarlas con las metas corporativas, estas a su vez con las metas relacionadas con TI y finalmente, estas relacionadas con los procesos catalizadores.

- Capítulo V. Plan de acción y plantillas.

  En este capítulo, se establecen dos resultados, el primero la hoja de ruta o plan de acción donde se define qué actividades y qué evidencias son necesarias para alcanzar un nivel deseado de capacidad de los procesos que resultaron prioritarios en el capítulo anterior; y el segundo, el desarrollo de productos entregables como plantillas, procedimientos, controles, manual, en estos productos se detallará los actores y las funciones para llevar a cabo la implementación de los mismos.

- Capítulo VI. Conclusiones y futuras líneas de investigación.

En la parte de las conclusiones del trabajo realizado como resultado de la elaboración de la tesis. También se destacan las principales aportaciones que realiza esta investigación.

En la parte final de la tesis, se presenta la referencia de la bibliografía que se ha empleado.

CAPÍTULO II

2 ESTADO DEL ARTE

En este capítulo, se presenta el estado del arte en el cual encaja el tema escogido, y para ello se profundiza en cuatro aspectos claves.

El primero, desarrollará un estado de arte en relación al Gobierno de Tecnologías donde se destaca definiciones de varios autores.

El segundo, desarrollará un estado de arte en relación a los principales marcos, estándares, guías, etc., más relevantes en la actualidad para el gobierno de TI como son COBIT5.0:2012 e ISO 38500 con el objetivo de presentar para cada una de las aproximaciones considerando los siguientes aspectos: definición y estructura.

El tercero, desarrollará un estado de arte en relación a la Gestión de Tecnologías donde se destaca definiciones de varios autores.

Finalmente, desarrollará un estado de arte en relación a los principales marcos, estándares, guías, etc., más relevantes en la actualidad para la gestión de TI como es ISO 27002, ITILV3 con el objetivo de presentar para cada una de las aproximaciones su problemática como: definición, estructura y aspectos varios a destacar.

2.1 GOBIERNO DE TI

En el ámbito del Gobierno de Tecnologías de la Información (IT Governance, el término en inglés), hay propuestas ampliamente aceptadas por la comunidad como Cobit5.0:2012, ISO38500:2015, Calder&Moir:2005, Forrester:2005. No obstante, para el objeto que aquí ocupa, sólo se consideran a continuación los más relevantes, significativos y característicos: ISO/IEC 38500:2015 y COBIT5.0:2012, en representación de Gobierno de TI. Para justificar por qué fueron considerados estos modelos se procede a aplicar el método MESME (Método de estudio de

similitud entre modelos y estándares) (J.Calvo-Manzano, G.Cuevas, M.Muñoz, & T.San Feliú, 2008) desarrollado por el grupo de investigación Cátedra para la Mejora de Procesos Software en el Espacio Iberoamericano de la Politécnica de Madrid quienes utilizaron como base para el proceso comparativo siete pasos de los cuales uno de ellos fue utilizado además como base para definir los criterios como se detalla a continuación:

Seleccionar estándares y modelos.

Como resultado de la revisión bibliográfica y la aplicación de criterios de búsqueda se seleccionaron dos estándares y/o modelos considerados más relevantes debido a que cumplen en alto grado los criterios establecidos. En la tabla se observa que se utilizó una ponderación cuyo significado esta dado de la siguiente manera:

1. Representa un alto grado de cumplimiento del criterio.
2. Represente un cumplimiento parcial del criterio.
3. Representa que no cumple el criterio satisfactoriamente.

Tabla 1. Estándares y modelos seleccionados.

Criterios	Cobit 5.0	ISO 38500	Calder&Moir	Forrester
1. El ámbito se basa en gobierno de TI	1	1	1	1
2. Proporciona información actualizada y se encuentra disponible	1	1	2	2
3. Relevancia de la institución proponente	1	1	2	2

Fuente: Propia

De acuerdo al resultado de la Tabla 1 se observa que Cobit5.0 e ISO 38500 son los que cumplen en alto grado el cumplimiento de todos los criterios.

El criterio 2 permite determinar qué modelos están actualizados y sin duda que tanto COBIT que en su última versión es 2012 y la iso38500 en el año 2015 son los más actualizados ya que CALDER&MOIR y FORRESTER su última actualización es 2005.

El criterio 3 establece que COBIT y la ISO38500 son respaldados por entidades muy importantes a nivel mundial como ISACA y por la International Organization for Standardization respectivamente mientras que CALDER&MOIR y FORRESTER son esfuerzos individuales.

2.1.1 ¿QUÉ ES EL GOBIERNO DE TI?

Se destaca algunas definiciones respecto al gobierno de TI, aunque existen muchas, se escogió las que más se adaptan para el contexto de este trabajo.

Según ISO IEC 38500:2008 Corporate Governance of Information Technology, "El Gobierno de las TI es el sistema a través del cual se dirige y controla la utilización de las TI actuales y futuras. Supone la dirección y evaluación de los planes de utilización de las TI que den soporte a la organización y la monitorización de dicho uso para alcanzar lo establecido en los planes de la organización. Incluye las estrategias y políticas de uso de las TI dentro de la organización."

Según Weill y Ross, 2004, "El Gobierno de las TI debe ocuparse de tres cuestiones: (i) Qué decisiones deben tomarse para asegurar la gestión y el uso efectivo de las TI (ii) Quiénes deben tomar estas decisiones (iii) Cómo serán ejecutadas y monitorizadas."

Según IT Governance Institute, 2003, "El Gobierno de las TI incluye las siguientes áreas: (i) La alineación entre la estrategia de la organización y de las TI, (ii)Obtención de valor que las TI generan para la organización (iii) Mecanismos que permitan mediciones apropiadas para poder valorar las TI en su conjunto y poder tomar decisiones respecto a su gobierno (iv) Gestión del riesgo que en un momento dado pueda afectar e impactar

negativamente en las actividades y procesos de la organización (v) Gestión de los recursos TI y la utilización óptima de los mismos."

Según Jorge Hidalgo, Gerente de Gestión y Gobierno TI de Mainsoft, un concepto simple, que es el que maneja este proveedor, es que "las TI de la empresa deben estar ordenadamente preparadas para apoyar al negocio en sus necesidades actuales y futuras, como minimizar riesgos, agregar valor y administrar adecuadamente los recursos tecnológicos".

Según Pablo Caneo, Presidente Capítulo Santiago de Chile de Isaca (Asociación de Auditoría y Control de Sistemas de Información), entidad que es referente en este tema. Él explica que Gobierno de TI "se define como una estructura de relaciones y procesos para dirigir y controlar la compañía hacia el logro de sus objetivos mediante la adición de valor, a la vez que mantiene un adecuado equilibrio entre riesgo y beneficio sobre TI y sus procesos".

Además es importante, establecer la relación entre el Gobierno Corporativo y el Gobierno de TI, el Gobierno Corporativo es un sistema mediante el cual las organizaciones son dirigidas y controladas, convirtiéndose en un aspecto importante en toda organización, ya que determina el desarrollo de las actividades, la consecución de objetivos generales y por ende, la consecución del éxito empresarial (Pedrosa Ortega, 2009) , el cual establece un conjunto de responsabilidades y prácticas ejecutadas por la junta directiva con los objetivos de proveer dirección estratégica (ECONOMICO, 2011). De esta manera, para dar cumplimiento a las estrategias y objetivos de la empresa se presenta el Gobierno de TI como parte integral del Gobierno Corporativo y consiste en el liderazgo, estructuras organizativas y procesos que aseguran el soporte de TI a la organización para dar cumplimiento a las estrategias y objetivos de la empresa (Haris Hamidovic, 2011) (Llorens, 2011).

2.1.1.1 RESUMEN DE GOBIERNO DE TI.

Luego de revisar los argumentos de varios autores del concepto de Gobierno de TI, se puede establecer que los criterios comunes respecto al gobierno de TI es que tiene cinco áreas claves, los cuales con una correcta administración pueden generar grandes beneficios; (1) alineamiento estratégico, (2) entrega de valor, (3) administración de riesgos, (4) administración de recursos y (5) medición del desempeño. También, indicar que el Gobierno de TI forma parte del gobierno empresarial, esto es que tecnología debe estar alineada a los objetivos institucionales; y por último se considera que se establece gobierno de TI cuando se es capaz de contestar a las siguientes interrogantes (i) ¿Cómo se toman las decisiones?, (ii)¿quienes toman las decisiones?, (iii)¿quiénes son los responsables? y (iv)¿Cómo los resultados de las decisiones son medidas y monitoreadas?.

En síntesis, el Gobierno de TI es el sistema a través del cual se dirige y controla la utilización de las TI actual y futura que permita que la TI apoyen a alcanzar los objetivos del negocio y se pueda minimizar riesgos, agregar valor y administrar adecuadamente los recursos tecnológicos.

2.1.2 ESTÁNDARES Y MODELOS DE GOBIERNO DE TI

2.1.2.1 COBIT 5.0.

COBIT (Objetivos de Control para Información y Tecnologías Relacionadas) es una “Guía para el gobierno y la gestión de TI, organizado para garantizar que los usos de los recursos de TI están efectivamente alineados con las estrategias de negocio de la organización” (Neto & Neto, 2013). Por otra parte, Laksono & Supriyadi, (2015) destaca que COBIT 5.0:2012 a diferencia de otros marcos de gobierno es el único constituido con varios estándares y mejores prácticas relacionadas con las TI, ya que integra todo el

conocimiento del marco de ISACA (Asociación de Auditoría y Control de Sistemas de Información) tales como (Val IT, Risk IT, BMI's, ITAF). Mientras que Tsai, Hsieh, Wang, Chen, & Li (2015), señala que éste marco "puede ayudar a la empresa a establecer objetivos y la estrategia del plan de gobierno de manera efectiva" permitiendo que la empresa alcance el objetivo final de crear valor para el negocio.

Actualmente Cobit5.0:2012, es un marco de trabajo que se enfoca en cinco principios fundamentales: (1) satisfacer las necesidades de las partes interesadas, (2) cubrir la empresa extremo a extremo, (3) aplicar un marco de referencia único integrado, (4) hacer posible un enfoque holístico y (5) separar el gobierno de la gestión. Para cubrir todos los aspectos de tecnologías en las empresas ha definido cinco procesos de gobierno y treinta y dos procesos de Tecnologías de Información para la gestión de TI" como se muestra en las Figuras 1 y 2, cada proceso está compuesto por prácticas (identificadas con verbos), en el caso de procesos de gobierno (evaluar, orientar y supervisar), y para el caso de procesos de gestión en 4 (cuatro) grandes ámbitos interrelacionados: Alinear, planificar y organizar (APO), construir, comprar e implementar (BAI), la entrega, servicio y soporte (DSS) y monitorear, evaluar y valorar (MEA), tal y como se muestra en la Figura 2 (ISACA, 2012). De acuerdo, a Gantman & Fedorowicz (2016) las organizaciones pueden no necesitar aplicar todos los procesos de COBIT, por lo tanto, éste marco de gobierno puede combinarse de manera que permita adaptarse a cada empresa.

El marco de trabajo fue desarrollado en Estados Unidos, por el Instituto de Governance TI / ISACA, el autor es Institute Governance TI y entre el historial de las publicaciones tenemos: Cobit 4.1:2007, siendo la última versión Cobit5.0, 2012.

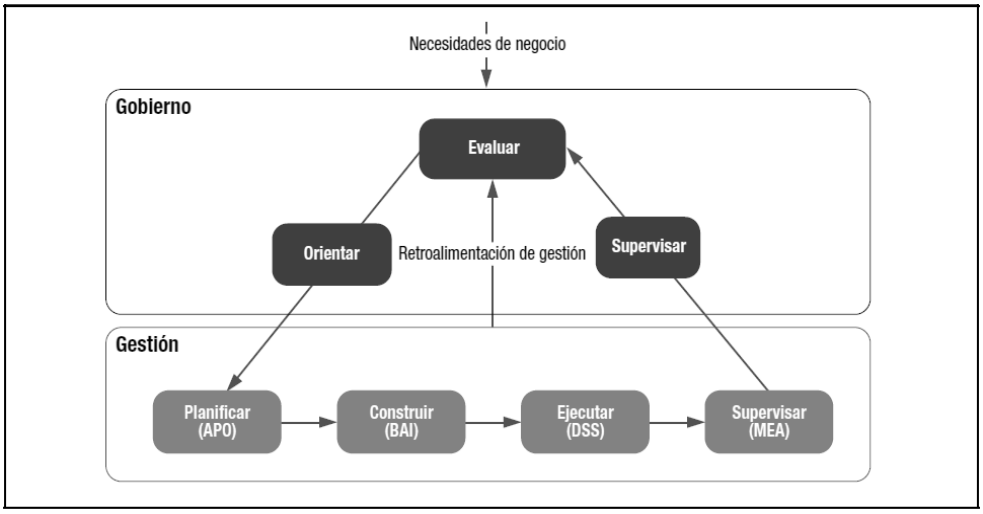


Figura 1. Áreas clave de Gobierno y Gestión de COBIT 5.0
Fuente: ISACA, (2012)

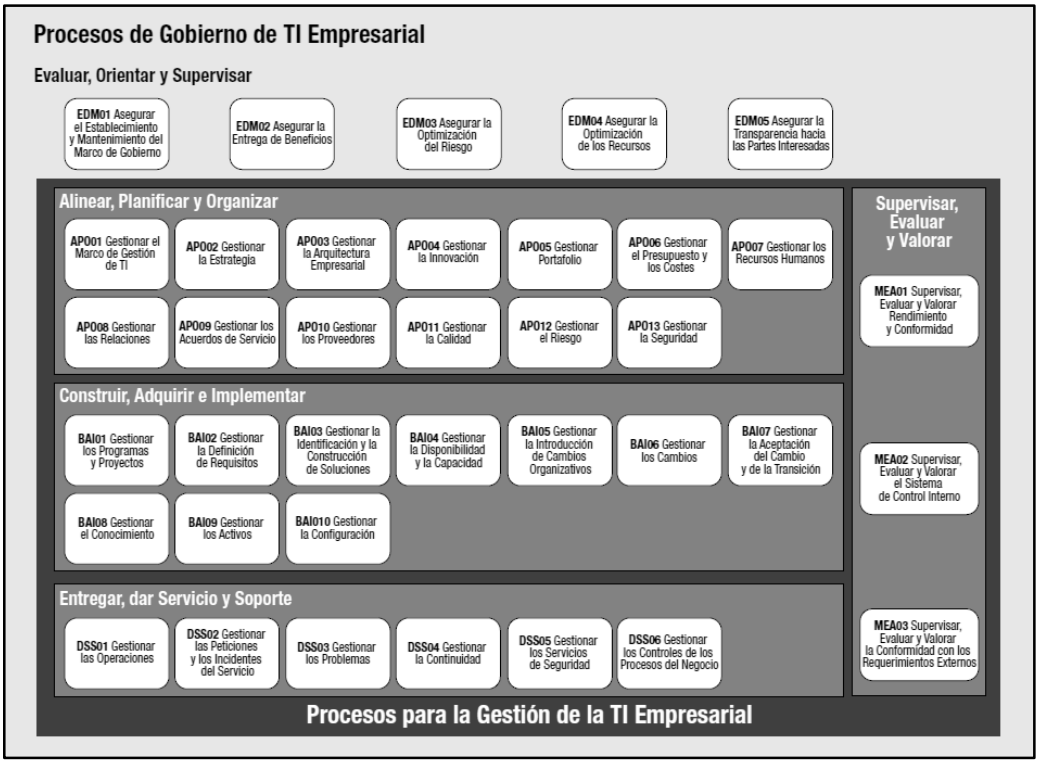


Figura 2. Procesos de Gobierno de TI Empresarial
Fuente: ISACA, (2012)

Continuando con la estructura de Cobit 5.0, información obtenida del libro de ISACA "Procesos catalizadores" (ISACA, 2012), se define que cada proceso (37 procesos) está compuesto por varias prácticas de gobierno, cada una de ellas tiene entradas, salidas y las actividades que

se deben realizar para cumplir las prácticas de gobierno, en el ejemplo se ilustran el proceso EDM01 cuya práctica de gobierno es el EDM01.01, y se muestra 5 actividades (ver Figura 3).

EDM01 Prácticas, actividades y entradas/salidas del Proceso

Práctica de gobierno	Entradas		Salidas	
	De	Descripción	Descripción	A
EDM01.01 Evaluar el sistema de gobierno. Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa.	MEA03.02	Comunicaciones de los requerimientos de cumplimiento modificados	Principios directrices del gobierno de la empresa	Todo EDM APO01.01 APO01.03
	Fuera del Ámbito de COBIT	• Tendencias en el entorno del negocio • Regulaciones • Gobierno/modelo de toma de decisiones • Constitución/normas/ estatutos de la organización	Modelo de toma de decisiones	Todo EDM APO01.01
			Niveles de autoridad	Todo EDM APO01.02

Actividades
1. Analizar e identificar los factores del entorno interno y externo (obligaciones legales, contractuales y regulatorias) y tendencias en el entorno del negocio que pueden influir en el diseño del gobierno.
2. Determinar la relevancia de TI y su papel con respecto al negocio.
3. Considerar las regulaciones externas, obligaciones legales y contractuales y determinar cómo deben ser aplicadas en del gobierno de TI de la empresa.
4. Alinear el uso y el procesamiento ético de la información y su impacto en la sociedad, en el entorno natural y en los intereses de las partes interesadas internas y externas con los objetivos, visión y dirección de la empresa.
5. Determinar las implicaciones del entorno de control conjunto de la empresa con respecto a TI.

Figura 3. Estructura de un proceso catalizador
Fuente: ISACA, (2012)

2.1.2.2 ISO 38500.

Según Chaudhuri (2011), la norma ISO/IEC 38500, es un estándar de asesoramiento para la Alta Dirección que se usa para la evaluación, dirección y monitoreo en el uso de las TI. Por otra parte, según Mohamad & Toomey (2016) la norma propone propósitos fundamentales de: (1) asegurar que los directivos puedan confiar en el gobierno corporativo de TI, (2) informar y orientar a los órganos del gobierno en el uso de las TI y (3) proporcionar una base de evaluación para el gobierno de TI.

Según ISO/IEC (2015), la norma se basa en la norma australiana AS8015:2005, y se encuentra alineada a los principios de gobierno recogidos en el "Informe Cadbury" y "Principios de Gobierno Corporativo de la OCDE", actualmente, la ISO 38500:2015, se enfoca en seis principios fundamentales: (1) Responsabilidades de la TI claramente definidas, (2) los planes estratégicos de la organización deben planear

que las TI satisfagan las necesidades del negocio actuales y futuras, (3) adquisición de TI de acuerdo a análisis apropiados, razones válidas, con decisiones claras y transparentes, (4) La calidad requerida de servicio es el adecuado para apoyar a la organización, permitiéndole satisfacer las necesidades del negocio, (5) las TI cumpla con todas las leyes, reglamentos, políticas definidas interna o externamente por la organización y (6) las políticas demuestren respeto por el comportamiento humano que labora dentro de la organización. Así mismo la norma presenta tres tareas principales: (1) evaluar el uso de las TI, (2) dirigir los planes y políticas que garanticen que las TI cumplan los objetivos, (3) y vigilar, supervisar y monitorear el uso y el cumplimento de las obligaciones (ver Figura 4).

El marco de trabajo fue desarrollado en la Unión Europea, por el International Organization for Standardization – ISO, su primera edición se publicó en junio del 2008 y su edición actual es la pública en el 2015.

En la siguiente figura se muestra el modelo de gobierno de TI.

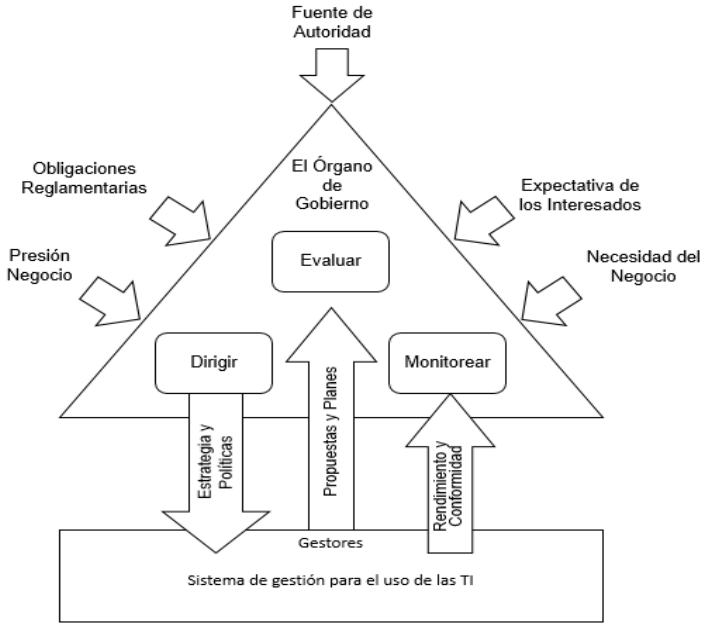


Figura 4. Modelo de Gobierno de TI
Fuente: ISO/IEC (2015)

La norma ISO/IEC (2015) describe actividades para cada principio en las tres tareas del modelo de gobierno de TI como se muestra en la Tabla 2.

	Evaluar	**Dirigir**	**Monitorear**
Responsabilidad	Asignación de responsabilidades relacionadas con el uso actual y futuro de la TI, y la evaluación de competencias de aquellos responsables de la toma de decisiones de la TI.	Dirigir las estrategias con las responsabilidades asignadas a TI y la recepción de información para cumplir responsabilidades y rendición de cuentas.	Mecanismos apropiados para el gobierno de TI, individuos que entiendan y asuman con sus responsabilidades asignadas, y desempeño de los responsables del gobierno de TI.

	Evaluar	Dirigir	Monitorear
Estrategia	EL órgano de gobierno debe encargarse de evaluar la evolución de TI y los procesos de negocio para asegurarse de que se proporcionara apoyo a las futuras necesidades de negocio, considerando los planes y políticas, se debe evaluar el uso de las TI y las actividades de TI, para asegurar que se alinean con los objetivos de la organización y satisfacer los requisitos de las partes interesadas. El órgano de gobierno también debería tener en cuenta las buenas prácticas. El órgano de gobierno debe garantizar que el uso de las TI está sujeto a gestión de riesgos adecuada.	El órgano de gobierno debe dirigir la preparación y el uso de estrategias y políticas que garanticen que la organización se beneficia de la evolución de las TI, también deben fomentar la presentación de propuestas para usos innovadores de la misma que permitan a la organización responder a nuevas oportunidades o desafíos, emprender nuevos negocios o mejorar los procesos.	EL órgano de gobierno debe supervisar el progreso de las propuestas que aprobó para asegurar que están alcanzando objetivos en plazos requeridos utilizando los recursos asignados, además deben vigilar el uso de TI para asegurarse de que está alcanzando sus beneficios previstos.
Adquisición	EL órgano de gobierno debe evaluar las opciones de TI, equilibrando los riesgos y la rentabilidad de las inversiones propuestas y aprobadas.	El órgano de gobierno debe ordenar que los activos de TI se adquieran de forma adecuada, garantizando que se cumplan con las capacidades requerida, especificadas en la documentación adecuada, todos estas adquisiciones deben apoyar las necesidades de negocio de la organización. El órgano de gobierno debe ordenar que la organización y los proveedores se comprometan en la toma de cualquier adquisición de TI.	El órgano de gobierno debe controlar las inversiones de TI para asegurar que proporcionan las capacidades requeridas

	Evaluar	Dirigir	Monitorear
Rendimiento	El órgano de gobierno deben evaluar los planes propuestos por los administradores para asegurar que se apoyará los procesos del negocio con la capacidad y la competencia requerida. Estas propuestas deben abordar la continuidad de la operación normal de la organización y el tratamiento del riesgo asociado con el uso de las TI. El órgano de gobierno debe evaluar los riesgos de continuidad del funcionamiento del negocio derivado de las actividades de TI, además debe evaluar los riesgos para la integridad de la información y la protección de los activos TI. El órgano de gobierno deben evaluar las opciones para asegurar tomas de decisiones eficaces y oportunas sobre el uso de las TI en apoyo de los objetivos de negocio. El órgano de gobierno debe evaluar regularmente la eficacia y el rendimiento de la organización del gobierno de TI.	El órgano de gobierno debe garantizar la asignación de recursos suficientes para que cumpla con las necesidades de la organización, de acuerdo con las prioridades acordadas y las limitaciones presupuestarias. El órgano de gobierno debe dirigir a los responsables para asegurarse de que es compatible con la organización, además de cuando sea requerido por razones de negocios, se presente información correcta y actualizada de datos que está protegido de la pérdida o mal uso.	El órganos de gobierno debe supervisar la medida en que se apoya el negocio, además de vigilar el grado en que la asignación de recursos y presupuestos se priorizan de acuerdo con los objetivos del negocio. El órgano de gobierno debe controlar el grado en que las políticas, tales como la exactitud de los datos y el uso eficiente de las TI, se siguen correctamente.
Conformidad	Evaluar periódicamente la medida en que satisfacen las obligaciones, políticas internas, normas y directrices, además debe evaluar el cumplimiento interno del marco de gobierno de TI.	EL órgano de gobierno debe dirigir a los responsables de establecer mecanismos regulares y de rutina para asegurar el uso de TI cumpla con obligaciones pertinentes, además de dirigir las políticas que se establecen y hacer cumplir, permitiendo que la organización cumpla con sus obligaciones internas. El órgano de TI debe disponer e personal de TI con directrices relevantes para el comportamiento profesional y desarrollo.	El órgano de gobierno debe supervisar el cumplimiento de TI y la conformidad a través de una comunicación adecuada y prácticas de auditoria. El órgano de gobierno debe supervisar las actividades de TI, para asegurar del medio ambiente, privacidad de la organización, gestión estratégica y cumplimiento de obligaciones pertinentes.

	Evaluar	Dirigir	Monitorear
Factor Humano	El órgano de gobierno debe evaluar las actividades de TI para asegurar la identificación y la adecuada consideración de las conductas humanas.	Actividades de TI que coincidan con el factor humano identificado, la identificación y notificación de riesgos, oportunidades, problemas y preocupaciones en todo momento por cualquier individuo, la gestión de riesgos mediante políticas y procedimiento, y la comunicación de cada uno de los a los responsables de la toma de decisiones.	Actividades de TI para asegurar que el factor humano es pertinente y tenga la atención adecuada, y asegurar que las prácticas de trabajo sean consistentes con el uso apropiado de la TI.

Tabla 2. Actividades para cada principio en las tres tareas del modelo de gobierno de TI.
Fuente: ISO/IEC (2015)

2.2 GESTIÓN DE TI

En el ámbito de la Gestión de Tecnologías de la Información hay propuestas como ISO 27001:2015, PMBOK, ITIL v3, cada una de ella se especializa en un tema en particular, por ejemplo, gestión de la seguridad de la información, gestión de proyectos, gestión de servicios, respectivamente. No obstante, para el objeto que aquí ocupa, sólo se considera a continuación el más relevante para el contexto de este trabajo que es ISO 27002:2013 e ITIL v3.

2.2.1 ¿QUÉ ES GESTIÓN DE TI?

Se destaca algunas definiciones respecto a la gestión de TI, aunque existen muchas, se escogió las que más se adaptan para el contexto del presente trabajo.

Según ISACA (2012), la gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

Según Folgueras Marcos & Santiago Ramirez (2010), para expresar una definición de gestión de TI de forma clara y entendible es necesario enmarcarla en el contexto de gobierno de TI. En este sentido, mientras, el

gobierno de TI establece los objetivos de TI alineados al negocio que tiene que cumplir los recursos de TI, la gestión de TI consiste en gestionar de una manera eficaz los recursos de TI para cumplir los objetivos planteados en el gobierno. Para que la Tecnología aporte el máximo valor al negocio, es indispensable que tanto el gobierno como la gestión funcionen al máximo nivel posible.

2.2.2 ESTÁNDARES Y MODELOS DE GOBIERNO DE TI

2.2.2.1 ISO 27002:2013

Establece un marco para la gestión de la seguridad de la información en organizaciones de cualquier tamaño y sector, que ayude a garantizar la confidencialidad, integridad y disponibilidad de la información, adicionalmente, la norma ISO 27002 establece un conjunto de controles de seguridad de la información que sirven como guía para la mitigación de los riesgos apreciados durante el análisis de riesgos.

La norma desarrollada por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), los orígenes de la norma se remontan al año 1995 con la publicación por parte del BSI Británico de su norma Bs 7799 parte 1, que definía un código de buenas prácticas para la gestión de la seguridad de la información. En el año 1999 fue lanzada la segunda parte de la misma norma en la que se definió por primera vez los requisitos para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI, o ISMS en inglés). La organización ISO adoptó la primera parte de la norma para la publicación de la ISO 17799 en el año 2000. Finalmente, tras sucesivas actualizaciones de las normas por parte de ambas entidades, ISO publicó la ISO 27001 en el año 2005 y poco después se cambió el nombre de la ISO 17799 para pasar a denominarse ISO 27002.

La estructura de la norma está constituida por cláusulas: a) Política de la seguridad (1), b) Organización de la seguridad de la información, c)

Gestión de activos (2), d) Seguridad de los recursos humanos, e) Seguridad física y del entorno, f) Gestión de operaciones y comunicaciones, g) Control del acceso, h) Adquisición, desarrollo y mantenimiento de sistemas de información, i) Gestión de los incidentes de la seguridad de la información, j) Gestión de la continuidad del negocio, k) Cumplimiento (3).

Cada cláusula, de la norma está compuesto por varios controles, cada una de ellas tiene actividades que se deben realizar para cumplir el control.

2.2.2.2 ITIL V3

ITIL (Information Technology Infraestructure Library o Biblioteca de Infraestructura de Tecnologías de la Información) es un conjunto de "buenas prácticas" para la gestión de los servicios de Tecnología Informática.

ITIL nació en la década de 1980, a través de la Agencia Central de Telecomunicaciones y Computación del Gobierno Británico (Central Computer and Telecomunications Agency - CCTA), como un apartado gestión de los servicios, habiéndose ampliado el conjunto de "buenas prácticas" a gestión de la seguridad de la información, gestión de niveles de servicio, perspectiva de negocio, gestión de activos software y gestión de aplicaciones. En la actualidad ITIL pertenece al Oficina de Comercio Británico (Office of Government Commerce - OGC), pero puede ser utilizado para su aplicación libremente.

La última versión, denominada como ITIL v3 se dio en 2007, en esta versión, los elementos principales de ITIL están compuestos por 5 volúmenes: (1) ITIL v3 Service Strategy (SS), (2) ITIL v3 Service Design (SD), (3) ITIL v3 Service Operation (SO), (4) ITIL v3 Continual Service Improvement (CST), (5) ITIL v3 Service Transition (ST), quienes conforman el ciclo de vida de ITIL.

CAPÍTULO III

3 INFORMACIÓN INSTITUCIONAL

3.1 DESCRIPCIÓN GENERAL DE LA INSTITUCIÓN

La Universidad Técnica de Machala es una institución de educación superior, legítimamente fundada el 14 de abril de 1969, resuelto así por el entonces Congreso de la República (Decreto no. 69-04); está ubicada en la ciudad de Machala, provincia de El Oro, su campus principal está situado en la Av. 25 de Junio Km. 5 ½ vía Pasaje.

Misión

"La Universidad Técnica de Machala es una institución de educación superior orientada a la docencia, a la investigación y a la vinculación con la sociedad, que forma y perfecciona profesionales en diversas áreas del conocimiento, competentes, emprendedores y comprometidos con el desarrollo en su dimensión es económico, humano, sustentable y científico-tecnológico para mejorar la producción, competitividad y calidad de vida de la población en su área de influencia".

Visión

"Ser líder del desarrollo educativo, cultural, territorial, socio-económico en la región y el país".

Organigrama

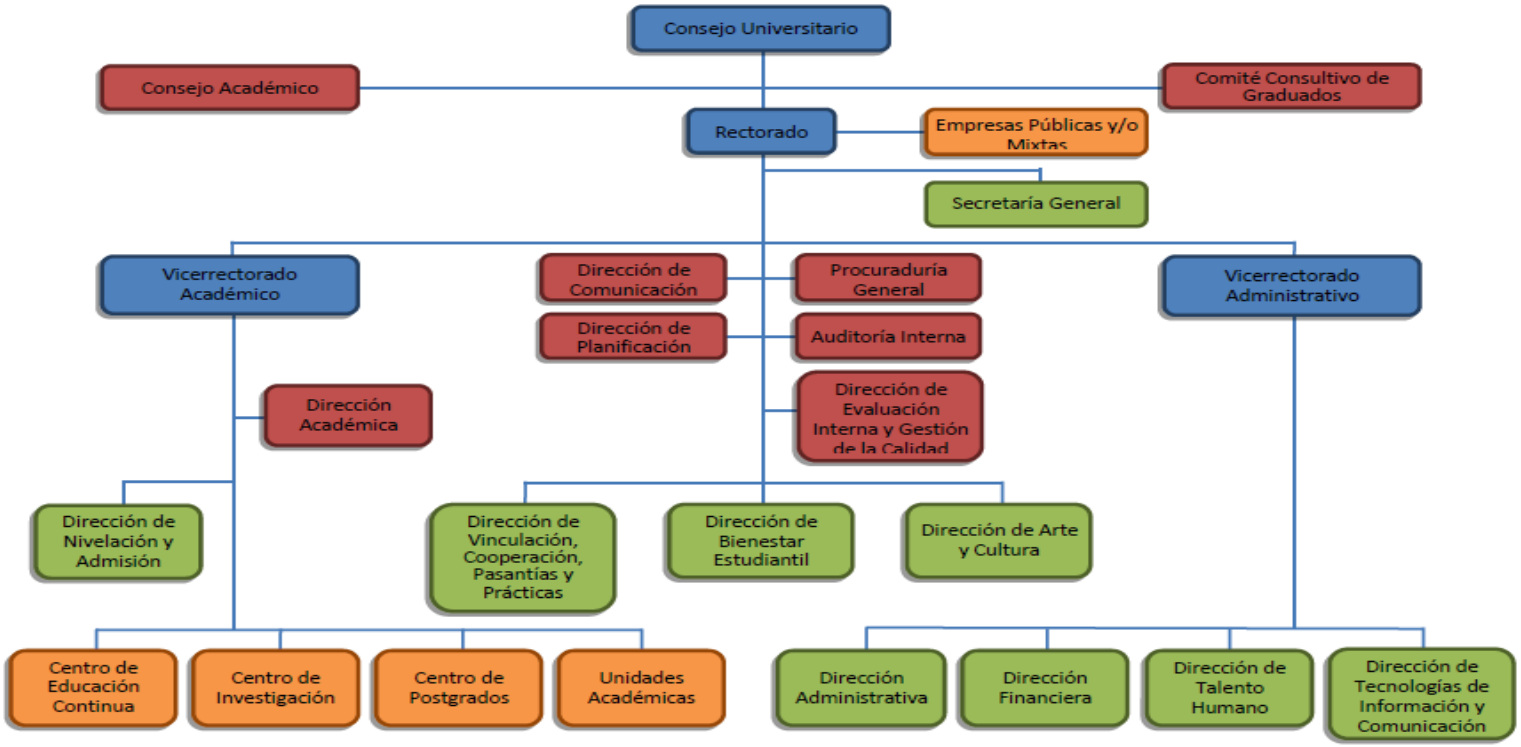


Figura 5.: Organigrama de la Universidad Técnica de Machala

Fuente: Universidad Técnica de Machala (2017)

3.2 ANTECEDENTES

La Universidad Técnica de Machala hasta el año 2010 realizó algunos de sus procesos más importantes manualmente, por ejemplo, no se contaba con un sistema de gestión académica, el apoyo de la informática se limitaba a un software de nómina y al mantenimiento del escaso hardware existente y de la ineficiente red de datos.

En el año 2008 las autoridades, considerando la importancia de los procesos informáticos para la universidad, deciden emprender en un proyecto de desarrollo de software y reingeniería de la infraestructura de red contando para esto con el apoyo de la unidad académica de informática con su carrera de ingeniería de sistemas, quienes destinaron a sus egresadas y egresados, además de sus docentes; así arranca el proyecto denominado SIUTMATCH (Sistema de Información de la Universidad Técnica de Machala).

La automatización de procesos en su fase inicial contempló el desarrollo de aplicaciones web integradas para la gestión académica como son: portal web institucional, inscripciones, matrículas, distributivos de asignaturas, notas, unidad de postgrado y aula virtual.

Así mismo se diseñó e implementó una nueva infraestructura de red, la primera fase contempló el tendido aéreo de fibra óptica el mismo que llega a todas las facultades del campus principal, se adquirieron y se configuraron dispositivos para el núcleo y parte de la distribución de la red, se contrató el servicio de acceso a internet con un ancho de banda de 550 Mbps, finalmente se realizó la compra de un servidor IBM Blade para dar soporte a las aplicaciones desarrolladas.

Hasta ese momento el recurso humano del departamento de informática estaba muy limitado en su número, así que para dar mantenimiento a las nuevas aplicaciones e infraestructura instalada se incorporaron cuatro nuevos empleados, quienes fueron seleccionados por participar desde el nacimiento del proyecto.

Actualmente se siguen desarrollando aplicaciones que se van integrando al SIUTMACH, otras son modificadas dependiendo de los requerimientos de los usuarios.

En infraestructura los requerimientos de hardware son cada vez mayores, a tal punto que el servidor adquirido inicialmente presentó problemas de procesamiento y almacenamiento, razón por la que contrataron el servicio de alojamiento en la nube para las aplicaciones críticas.

En una segunda fase relacionada con la infraestructura de red construyeron y adecuaron una nueva área física para el núcleo de la red, adquirieron y pusieron en marcha un sistema de alimentación eléctrica ininterrumpida y una planta generadora, en este nuevo espacio se encuentran actualmente los equipos del núcleo de la red.

3.3 PROBLEMÁTICA

El desarrollo de nuevas aplicaciones, la implementación de infraestructura y la incorporación de personal, hacen que la Dirección de TI esté cada vez más expuesto a amenazas sean éstas: naturales, intencionales o involuntarias.

Conforme pasa el tiempo y la Dirección de TI crece, estas amenazas son cada vez mayores junto con la probabilidad de que las mismas exploten los puntos débiles no detectados y no controladas. Si esto ocurriera, los elementos de valor de la Dirección de TI se verán afectados y por tanto causaría perjuicios a la organización.

Un aspecto sumamente crítico se vivió en 2010 cuando el servidor que alojaba el sistema de gestión académica de la Universidad colapsara haciendo el proceso de matrícula sumamente lento y en varios casos interrumpiéndolo, generando molestias en el colectivo estudiantil.

Desafortunadamente la exposición a las amenazas y la carencia de salvaguardas es desconocida por los directivos de la Universidad y la gerencia de TI tiene poco

conocimiento para poder afrontar la situación, a esto se debe sumar el poco esmero para la administración de los riesgos tecnológicos.

El desconocimiento y por tanto la falta de compromiso por parte de las autoridades y la Dirección de TI pone en riesgo la seguridad de los activos particularmente de la información. De igual manera si no se controlan de forma adecuada sea el software, el hardware o el personal las operaciones del negocio se pueden ver gravemente afectadas.

Aunque por políticas de gobierno se ha iniciado trabajos relacionados al cumplimiento del EGSI (Esquema Gubernamental de Seguridad de la Información) con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información.

3.4 DESCRIPCIÓN GENERAL DE LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

La Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Machala está adscrita al vicerrectorado administrativo cuya misión es fomentar la cultura informática y el aprovechamiento de las tecnologías de la información y de la comunicación dentro de la Institución y el responsable tiene la nominación de Directora o Director de Tecnologías de la Información y de la Comunicación, esta información es proporcionada por la UTMACH.

Funciones y atribuciones:

- Organizar, mantener y controlar los sistemas informáticos de la Universidad.
- Organizar, mantener y dirigir los procesos de automatización de la gestión de trámites institucionales.
- Dirigir la digitalización de la información institucional.
- Diseñar y dar soporte al portal web oficial de la institución.
- Administrar y mantener el buen funcionamiento de los sistemas de telecomunicación.

- Determinar políticas de uso de las tecnologías de la información y de la comunicación, en coordinación con la Dirección Administrativa y Dirección Académica.
- Proponer la creación y aplicación de nuevas herramientas basadas en las tecnologías de la información y de la comunicación tendente a automatizar todos los procesos de la UTMACH.
- Asesorar a las principales autoridades de la UTMACH en los temas relacionados con las tecnologías de la información y de la comunicación;
- Control y mantenimiento de la infraestructura de red de la UTMACH;
- Administración, custodia y mantenimiento del datacenter; y,
- Capacitar en el uso de las herramientas y programas informáticos a las autoridades y servidoras y servidores de la UTMACH.

Productos y Servicios:

- Sistemas informáticos.
- Infraestructura de red funcionando adecuadamente.
- Servicio de internet y telefonía.
- Informes de asesoría.
- Soporte a usuarios.
- Soporte técnico al portal web institucional; y,
- Talleres de capacitación. (Universidad Técnica de Machala, 2017)

Aunque en el departamento de TI de la Universidad Técnica de Machala las áreas, las tareas y responsabilidades no se encuentran formalizadas se puede identificar lo siguiente:

Área	Tareas y responsabilidades	Descripción
Gestión de T.I.	Soporte a usuarios	Asegurar que los problemas de los usuarios reciben una asistencia adecuada.
	Capacitación	Garantizar que los empleados y usuarios de los SI estén capacitados para usar y gestionar la T.I.
	Gestión	Gestionar y controlar todos los aspectos de la organización de TI, sus unidades y sus recursos.
Desarrollo de software	Creación de aplicaciones	Se desarrollan nuevas aplicaciones siguiendo las fases de análisis, diseño, desarrollo, pruebas e implementación.
	Mantenimiento de aplicaciones	Dependiendo de las necesidades de los usuarios se efectúan cambios en las aplicaciones ya creadas e implementadas, así mismo se corrigen errores.
	Capacitación de los usuarios	Cada vez que se crea un software se capacita al usuario para su correcta utilización
	Datos	Diseño, desarrollo y preparación de los aspectos técnicos, archivos, procedimientos para gestionar los sistemas de información. Respaldos de las bases de datos
Infraestructura de red y sistemas operativos	Reestructuración y mantenimiento a la infraestructura de red	Estudios de requerimientos para la implementación de nuevos servicios.
		Adecuaciones a la red de datos dependiendo del crecimiento de esta.
		Respaldo de Configuraciones de equipos esenciales.
		Mantenimiento preventivo y correctivo de los dispositivos de red.
	Mantenimiento y configuración de los sistemas operativos	Actualización de las versiones de sistemas operativos
		Actualización de los paquetes de aplicación del servidor.
Mantenimiento	Soporte técnico	Mantenimiento preventivo y correctivo a las computadoras de usuario final

Tabla 3. Áreas y responsabilidades del departamento de TI de la UTMACH
Fuente: Universidad Técnica de Machala (2017)

La Dirección de TI cuenta con una directora encargada, ella es responsable de la Gestión de las Tecnologías de Información, cuatro analistas/programadores asignados al área de desarrollo de software, un administrador para la infraestructura de red y un técnico para mantenimiento.

3.5 FODA DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.

La Dirección de TI en reuniones con su personal estableció en forma general esta matriz que muestra las fortalezas, oportunidades, debilidades y amenazas que refleje en forma macro las preocupaciones de esta entidad. Indicar que esta matriz permanece desde el año 2012 y no ha sido actualizada.

FORTALEZAS	**OPORTUNIDADES**
• Equipo Humano equilibrado en cuanto a sus capacidades • Predisposición a realizar los cambios necesarios • Disponer de personal para desarrollo de los sistemas de la institución	• Lograr que el área de tecnología sea considerada no como apoyo sino como estratégico en la consecución de la acreditación.
DEBILIDADES	**AMENAZAS**
• La Dirección de Tecnología de la Información no es una unidad de asesoría en la toma de decisiones, todavía continúa sintiéndose como una unidad de apoyo en la ejecución • Por la fecha de cumplimiento para la acreditación los proyectos se establecen en base a necesidades de lo que exige el CEAACES y no en base a estudio de análisis de riesgos u otra estrategia para generar proyectos. • Para el servicio de internet 100% se depende de una empresa proveedora • No tener aprobado un plan para administrar riesgos • No tener aprobado una estructura y plan para administrar la seguridad de la información	• Falta de una normativa adecuada que logre regular adecuadamente los procesos que desarrolla la Dirección de Tecnología de la Información.

• No Tener implementado procesos en base a una norma sino, de forma empírica.	

Tabla 4: Matriz FODA
Fuente: UTMACH

3.6 DIAGNÓSTICO DE PROCESOS MEDIANTE EL NIVEL DE CAPACIDAD DE LOS PROCESOS

En este capítulo, se plantea como objetivo establecer el nivel de capacidad de los procesos utilizando el modelo que propone el marco de trabajo COBIT 5.0 (cinco procesos de gobierno de TI y treinta y dos procesos de gestión de TI) en la Universidad Técnica de Machala, en este sentido, se planifico realizar las siguientes actividades:

1 Revisión literaria respecto al modelo de Evaluación de procesos que plantea COBIT 5.0.
2 Explicación de la estrategia para aplicar la herramienta de investigación en la Universidad Técnica de Machala.
3 Resultados Obtenidos.

3.6.1 REVISIÓN LITERARIA RESPECTO AL MODELO DE EVALUACIÓN DE PROCESOS QUE PLANTEA COBIT 5.0

COBIT 5.0 tiene un Modelo de Evaluación de Procesos (PAM por sus siglas en inglés de Process Assessment Model), el cual permite establecer un análisis de situación actual de los procesos de gobierno y gestión de Tecnologías de la Información y su nivel de capacidad, basado en la norma internacional ISO / IEC 15504 de Ingeniería de Software-Evaluación de Procesos (ISACA, PAM-Using cobit 5 Toolkit-tkt_eng_0114, 2016), el modelo busca apoyar a la mejora de procesos a través de medidas del desempeño de los mismos.

Para explicar el funcionamiento del Modelo de Evaluación de procesos (PAM), considere primero detallar los elementos que forman parte del modelo, y luego explicar la integración de los mismos mediante un diagrama que refleje la secuencia de las actividades que se deben ir realizando.

3.6.1.1 ELEMENTOS DEL MODELO DE EVALUACIÓN DE PROCESOS

El modelo plantea el uso de seis niveles (0 al 5) de capacidad que se pueden alcanzar para cada proceso (NETWORK, 2011).

NIVELES DE CAPACIDAD

Nivel 0 Proceso Incompleto: El proceso no está implementado o no alcanza su propósito, en este nivel hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso. Nivel 1 Proceso Ejecutado (un atributo) El proceso implementado alcanza su propósito. Nivel 2 proceso Gestionado (dos atributos) El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificada, supervisada y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente. Nivel 3 Proceso Establecido (dos atributos) El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso. Nivel 4 Proceso predecible (dos atributos) El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso. Nivel 5 Proceso optimizado (dos atributos) El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas empresariales presentes y futuras.
Cada nivel de capacidad puede ser alcanzado sólo cuando el nivel inferior se ha alcanzado por completo. Para llevar a cabo una evaluación con el modelo de capacidad de los procesos de COBIT 5.0, hay que distinguir entre evaluar el nivel 1 de capacidad y los niveles superiores, debido que el nivel 1 de capacidad de procesos describen para cada proceso si ha alcanzado su objetivo establecido, siendo este base para hacer alcanzables los niveles de capacidad superiores.

Tabla 5. Niveles de capacidad de los procesos catalizadores
Fuente: ISACA (2012)

ESCALA DE VALORACIÓN.

Los rangos definidos para la evaluación de capacidad de los procesos se basan también en las escalas y rangos de la norma ISO/IEC 15504 de acuerdo al grado en el que cada objetivo es alcanzado.

Esta escala consiste en los siguientes ratios:

N (No alcanzado) Hay muy poca o ninguna evidencia de que se alcanza el atributo definido en el proceso de evaluación (0al 15 por ciento de logro)
P (Parcialmente alcanzado) Hay alguna evidencia de aproximación a, y algún logro del atributo definido en el proceso evaluado. Algunos aspectos del logro del atributo pueden ser impredecibles (15 a 50 por ciento de logro).
L (Ampliamente alcanzado) Hay evidencias de un enfoque sistemático y de un logro significativo del atributo definido en el proceso evaluado. Pueden encontrarse algunas debilidades relacionadas con el atributo en el proceso evaluado. (50 a 85 por ciento de logro)
F (Completamente alcanzado) Existe evidencia de un completo y sistemático enfoque y un logro completo del atributo definido en el proceso evaluado. No existen debilidades significativas relacionadas con el atributo en el proceso evaluado (85 a 100 por ciento de logro)

Tabla 6. Escala de valoración.
Fuente: ISACA (2012)

ATRIBUTOS DE CAPACIDAD DE PROCESOS.

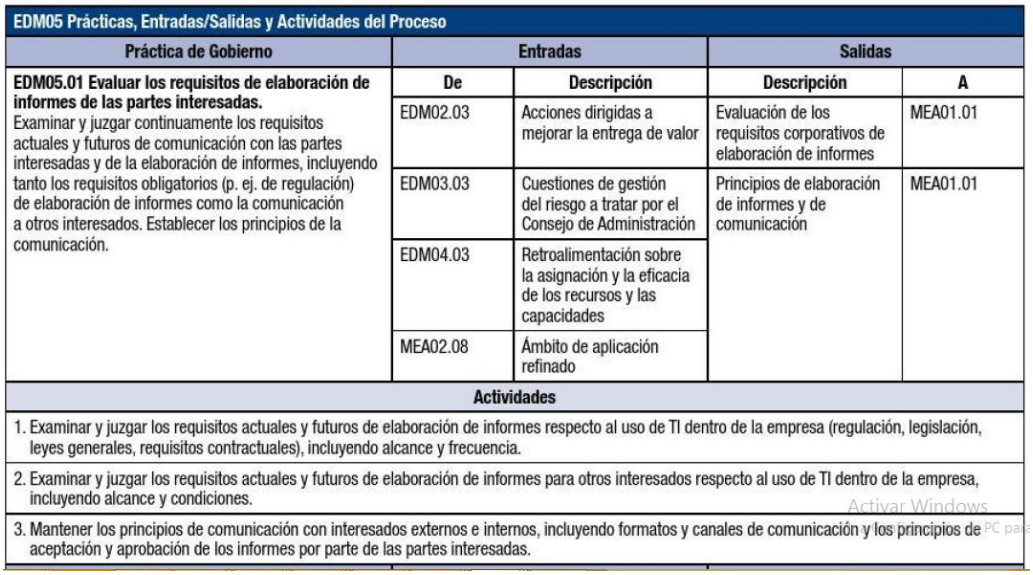
La medición de la capacidad se basa en un conjunto de atributos del proceso. Cada atributo define un aspecto particular de la capacidad del proceso.
Cada nivel de capacidad tiene definido atributos, siendo un total de 9 atributos.

Nivel 0	No tiene atributos
Nivel 1	PA 1.1 El proceso implementado alcanza sus propósitos
Nivel 2	PA 2.1 Administración del desempeño PA 2.2 Administración del producto del trabajo
Nivel 3	PA 3.1 Definición del proceso PA 3.2 Desarrollo del proceso
Nivel 4	PA 4.1 Medición del proceso PA 4.2 Control del proceso
Nivel 5	PA 5.1 Innovación del proceso PA 5.2 Optimización del proceso

Tabla 7. Atributos de capacidades de procesos
Fuente: ISACA (2012)

Como se muestra en la Tabla 7 de atributos de Capacidad de procesos, cada nivel de capacidad tiene atributos por cumplir y estos tienen **Indicadores** que permiten verificar el cumplimiento. A continuación, se explica cómo se aplica los indicadores para cada nivel de capacidad.

Para el Nivel 1, es necesario explicar cómo COBIT 5.0 estructura la información para cada proceso observado en el libro de procesos catalizadores de COBIT5 (ISACA, procesos catalizadores, 2012), como ilustra la Figura 6 se puede notar que cada proceso por ejemplo EDM05 tiene Practica de Gobierno (EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas) y tiene Entradas, Salidas, Actividades por realizar, luego de revisar la información de cada proceso, ISACA PAM-Using cobit 5 Toolkit-tkt_eng_0114 (2016) manifiesta que para el nivel 1 el Modelo de Evaluación de procesos utiliza las prácticas de gobierno , las entradas y salidas de cada proceso como se ilustra en la Figura 6.



EDM05 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gobierno	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas. Examinar y juzgar continuamente los requisitos actuales y futuros de comunicación con las partes interesadas y de la elaboración de informes, incluyendo tanto los requisitos obligatorios (p. ej. de regulación) de elaboración de informes como la comunicación a otros interesados. Establecer los principios de la comunicación.	EDM02.03	Acciones dirigidas a mejorar la entrega de valor	Evaluación de los requisitos corporativos de elaboración de informes	MEA01.01
	EDM03.03	Cuestiones de gestión del riesgo a tratar por el Consejo de Administración	Principios de elaboración de informes y de comunicación	MEA01.01
	EDM04.03	Retroalimentación sobre la asignación y la eficacia de los recursos y las capacidades		
	MEA02.08	Ámbito de aplicación refinado		
Actividades				
1. Examinar y juzgar los requisitos actuales y futuros de elaboración de informes respecto al uso de TI dentro de la empresa (regulación, legislación, leyes generales, requisitos contractuales), incluyendo alcance y frecuencia.				
2. Examinar y juzgar los requisitos actuales y futuros de elaboración de informes para otros interesados respecto al uso de TI dentro de la empresa, incluyendo alcance y condiciones.				
3. Mantener los principios de comunicación con interesados externos e internos, incluyendo formatos y canales de comunicación y los principios de aceptación y aprobación de los informes por parte de las partes interesadas.				

Figura 6. Proceso catalizador EDM05.01

Fuente: ISACA, procesos catalizadores (2012).

Práctica Genérica BPS	Ej. EMD01 – edm01.01, edm01.02, edm01.03 Prácticas de Gobierno
Producto de Trabajo Genérico WPS	Las entradas y salidas de cada proceso

Tabla 8. Representación de los elementos a considerar en el nivel 1
Fuente: Propio

Para el Nivel 2 en adelante se aplica indicadores genéricos propuestos por la ISO 15504 preestablecidos como se muestra en la Tabla 9, la distribución de los atributos se muestra en la Tabla 7 de atributos de capacidad de procesos.

Nivel 2 Administrador	**PA 2.1 Gestión del rendimiento-desempeño – Medida del nivel de gestión del rendimiento del proceso.**	**Como resultado del logro completo de este atributo:**
		A) Se identifican los objetivos para el desempeño del proceso.
		B) Se planifica y supervisa el desempeño del proceso.
		C) El desempeño del proceso se ajusta a los planes.
		D) Las responsabilidades y autoridades para realizar el proceso se definen, asignan y comunican.

		E) Los recursos e información necesarios para llevar a cabo el proceso son identificados, puestos a disposición, asignados y utilizados.
		F) Las interfaces entre las partes involucradas se gestionan para asegurar una comunicación efectiva y también una clara asignación de responsabilidades.
	PA 2.2 Gestión del producto de trabajo. Una media en que los productos de trabajo producidos por el proceso se gestionan adecuadamente. Los productos de trabajo (entradas o salidas del proceso) son definidos y controlados.	Como resultado del logro completo de este atributo:
		A) Se definen los requisitos para los productos de trabajo del proceso.
		B) Se definen los requisitos para la documentación y control de los productos de trabajo.
		C) Los productos de trabajo están debidamente identificados, documentados y controlados.
		D) Los productos de trabajo se revisan de acuerdo con las disposiciones planificadas y se ajustan según sea necesario para cumplir con los requisitos.
Nivel 3 Establecido	PA 3.1 Definición del proceso. Una medida en que se mantiene un proceso estándar para apoyar el despliegue del proceso definido	Como resultado del logro completo de este atributo:
		A) Se define un proceso estándar, incluyendo pautas apropiadas de adaptación, que describe los elementos fundamentales que deben ser incorporados en un proceso definido.
		B) Se determina la secuencia e interacción del proceso estándar con otros procesos.
		C) Las competencias y funciones necesarias para realizar un proceso se identifican como parte del proceso estándar.
		D) La infraestructura requerida y el ambiente de trabajo para realizar un proceso se identifican como parte del proceso estándar.
		E) Se determinan métodos adecuados para controlar la eficacia y la idoneidad del proceso.
	PA 3.2 Despliegue de procesos. Una medida en que el proceso estándar se despliega efectivamente como un proceso definido para lograr los resultados de su proceso.	Como resultado del logro completo de este atributo:
		A) Se despliega un proceso definido sobre la base de un proceso normalizado adecuadamente seleccionado y / o adaptado.
		B) Se asignan y comunican las funciones, responsabilidades y autoridades necesarias para realizar el proceso definido.
		C) El personal que realiza el proceso definido es competente sobre la base de una educación, capacitación y experiencia apropiadas.

		D) Los recursos necesarios y la información necesaria para realizar el proceso definido se ponen a disposición, se asignan y se utilizan.
		E) La infraestructura necesaria y el entorno de trabajo para realizar el proceso definido se ponen a disposición, se gestionan y se mantienen.
		F) Se recopilan y analizan los datos apropiados como base para comprender el comportamiento y para demostrar la idoneidad y eficacia del proceso y para evaluar dónde se puede mejorar continuamente el proceso.
Nivel 4 Previsible	PA 4.1 Medición del proceso. Una medida en que se usan los resultados de las mediciones para asegurar que el desempeño del proceso apoya el logro de los objetivos de desempeño del proceso relevantes en apoyo de los objetivos de negocio definidos	Como resultado del logro completo de este atributo:
		A) Se establecen las necesidades de información de proceso en apoyo de las metas de negocio definidas relevantes.
		B) Los objetivos de medición del proceso se derivan de las necesidades de información del proceso.
		C) Se establecen objetivos cuantitativos para el desempeño del proceso en apoyo de los objetivos empresariales pertinentes.
		D) Las medidas y la frecuencia de medición se identifican y definen de acuerdo con los objetivos de medición del proceso y los objetivos cuantitativos para el desempeño del proceso.
		E) Los resultados de las mediciones se recopilan, analizan y reportan con el fin de monitorear hasta qué punto se cumplen los objetivos cuantitativos para el desempeño del proceso.
		F) Los resultados de la medición se utilizan para caracterizar el rendimiento del proceso.
	PA 4.2 Control de Proceso. Una medida en que el proceso se gestiona cuantitativamente para producir un proceso que es estable, capaz y predecible dentro de límites definidos.	Como resultado del logro completo de este atributo
		a) Las técnicas de análisis y control se determinan y aplican cuando procede.
		b) Se establecen límites de variación de control para el rendimiento normal del proceso.
		c) Los datos de medición se analizan para determinar las causas especiales de variación
		d) Se toman medidas correctivas para abordar causas especiales de variación.
		e) Los límites de control se restablecen (según sea necesario) después de la acción correctiva

Nivel 5 Optimizado.	PA 5.1 Innovación de procesos - Una medida que los cambios en el proceso se identifican a partir del análisis de causas comunes de variación en el desempeño y de investigaciones de enfoques innovadores para la definición y despliegue del proceso.	Como resultado del logro completo de este atributo:
		A) Se definen los objetivos de mejora del proceso para el proceso que apoyan los objetivos empresariales relevantes.
		B) Se analizan datos apropiados para identificar causas comunes de variaciones en el desempeño del proceso.
		C) Se analizan datos apropiados para identificar oportunidades de mejores prácticas e innovación.
		D) Se identifican las oportunidades de mejora derivadas de las nuevas tecnologías y conceptos de proceso.
		E) Se establece una estrategia de implementación para lograr los objetivos de mejora del proceso.
	PA 5.2 Optimización del proceso - Una medida en que los cambios en la definición, la gestión y el desempeño del proceso producen un impacto efectivo que logra los objetivos relevantes de mejora del proceso.	Como resultado del logro completo de este atributo:
		A) El impacto de todos los cambios propuestos se evalúa en función de los objetivos del proceso definido y del proceso estándar.
		B) La implementación de todos los cambios acordados se gestiona para asegurar que cualquier interrupción en el desempeño del proceso se entienda y actúe.
		C) Sobre la base del desempeño real, se evalúa la efectividad del cambio del proceso en función de los requisitos definidos del producto y los objetivos del proceso para determinar si los resultados se deben a causas comunes o especiales.

Tabla 9. Representación de los indicadores genéricos propuestos por la ISO 15504 a considerar en los niveles 2 hasta el nivel 5
Fuente: ISACA, Cobit 5.0 Self Assessment Templates en español (2013).

3.6.1.2 INTEGRACIÓN DE LOS ELEMENTOS DEL MODELO DE EVALUACIÓN DE PROCESOS.

Una vez que se expuso los elementos del modelo de evaluación de procesos (PAM), se ha considerado necesario diseñar un diagrama de flujo que refleje la secuencia de actividades que se debe realizar para obtener el nivel de capacidad de los procesos de COBIT5.0, el cual refleje la integración de los elementos mencionados.

En este sentido, en la Figura 7 mostrada más adelante, se resalta con un círculo una numeración como referencia en la siguiente explicación.

Círculo 1. Establecer los indicadores de atributo para el Nivel 1.

- **Definir los procesos de gobierno (Bps).**
- **Definir producto de trabajos genéricos (Wps)**

Para esta actividad se ha tomado del libro procesos catalizadores de COBIT 5.0 las prácticas de gobierno/gestión (Bps) por cada proceso, considere que, para alcanzar mayor nivel de detalle, aplicar las actividades por cada práctica de gobierno/gestión que propone el libro antes mencionado, debido a que cada actividad es muy abarcadora, esto es en una misma actividad establece sub-actividades implícitamente, y al momento de aplicar la auditoría de cumplimiento el entrevistado se complicaría en su respuesta(no sabría si contestar en parte, si/no), entonces, por cada una de ellas se ha generado preguntas con el objetivo de desagregar las sub-actividades implícitas, se ilustra en la Tabla 10 un ejemplo con el proceso EDM01. Esta actividad se la realizo para los cinco procesos de gobierno y 29 procesos de gestión, no se consideró los 3 procesos del dominio Supervisar, Evaluar y Valorar porque la institución manifestó que para ellos no se tiene ninguna evidencia del cumplimiento. Los anexos de los 29 procesos incorpora la evidencia del cumplimiento de las actividades que escogieron que si cumplen, las mismas que se almacenó en una carpeta de google drive por lo cual se muestra el link https://goo.gl/dvb6Ne

Prácticas de gobierno/gestión (Bps)	**Actividades**	**Pregunta para evidenciar el cumplimiento de la actividad**	**[illegible] cumplen S/N**	**Comentario**	**Evidencia**
EDM01.01 EVALUAR EL SISTEMA DE GOBIERNO (Identificar y comprometerse continuamente con las partes	Analizar e identificar los factores del entorno interno y externo (obligaciones legales, contractuales y regulatorios) y tendencias en el entorno del negocio que puedan influir en el diseño del gobierno	¿Posee un listado de factores internos y externos que afecten al negocio?			
		Existe algún mecanismo documentado de aplicación de los factores que afectan a los			

Prácticas de gobierno/gestión (Bps)	Actividades	Pregunta para evidenciar el cumplimiento de la actividad	[illegible] cumplen S/N	Comentario	Evidencia
interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa		procesos de TI establecidos?			
	Determinar la relevancia de TI y su papel con respecto al negocio	Los procesos aplicados a TI ayudan a cumplir con los objetivos estratégicos de la empresa?			
		¿Se evidencia en algún documento la determinación de aspectos claves que mejoren el desempeño o el cumplimiento de los objetivos organizacionales gracias a las funciones TI?			
		¿Los procesos y materiales usados en el departamento de TI sirven para garantizar el funcionamiento adecuado del negocio?			
	Considerar las regulaciones externas, obligaciones legales y contractuales y determinar cómo deben ser aplicadas en el gobierno TI de la empresa.	¿Cumple con las leyes, regulaciones y compromisos contractuales con los que está comprometida la empresa?			
		¿Existe métricas para verificar el cumplimiento de las leyes, regulaciones y compromisos contractuales?			
	Alinear el uso y el procesamiento ético de la información y su impacto en la sociedad, en el entorno natural y en los intereses de las partes interesadas internas y externas con los objetivos, visión y dirección de la empresa	¿Se usa y se procesa de forma ética la información basado en una normativa estandarizada?			
	Determinar las implicaciones del entorno de control conjunto de la empresa con respecto a TI.	¿Existe un documento donde se especifiquen las políticas de TI relacionadas con el entorno de la empresa?			

Prácticas de gobierno/gestión (Bps)	Actividades	Pregunta para evidenciar el cumplimiento de la actividad	[illegible] cumplen S/N	Comentario	Evidencia
		¿Se satisface las necesidades de TI con respecto al entorno de control de la empresa?			
	Articular los principios que guiaran el diseño de la toma de decisiones sobre el gobierno de TI.	¿Posee un modelo que optimice la toma decisiones?			
	Comprender la cultura empresarial de la toma de decisiones y determinar de un modelo optimo en la toma de decisiones para TI.	¿Se analizó como se llevan a cabo la toma de decisiones de la empresa?			
		¿Se implementó un modelo de toma de decisiones TI basado en el modelo de toma de decisiones de la empresa?			
	Determinar los niveles apropiados para la delegación de autoridad, incluyendo reglas de umbrales, para las decisiones de TI.	¿Se define en el modelo de toma de decisiones niveles para delegación de autoridad?			
EDM01.02 Orientar el sistema de gobierno Informar los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios modelos para la toma de decisiones y	Comunicar los principios del gobierno de TI y acordar con el gestor ejecutivo la manera de establecer un liderazgo informado y comprometido	¿Existe alguna documentación que evidencie los principios del gobierno de TI?			
		¿Socializa sus funciones y proyectos con el gestor ejecutivo para las pertinentes aprobaciones?			
	Establecer o delegar el establecimiento de las estructuras, procesos y prácticas del gobierno en línea con los principios de diseño acordados	¿Existe un documento donde este establecidas las estructuras, procesos y prácticas del gobierno IT?			
		¿Existe un departamento o un encargado de establecer estructuras y procesos así como de la optimización de los mismos?			

Prácticas de gobierno/gestión (Bps)	Actividades	Pregunta para evidenciar el cumplimiento de la actividad	[illegible] cumplen S/N	Comentario	Evidencia
niveles de autoridad diseñados para el gobierno. Definir la información necesaria para una toma de decisiones informadas.	Asignar responsabilidades, autoridad y la responsabilidad de que se apliquen los principios de diseños de gobierno, los modelos de toma de decisión y de delegación acordados.	¿La organización posee un documento donde se define funcionalidades y responsabilidades de los empleados?			
	Garantizar que los mecanismos de notificación y de comunicación proporcionan información adecuada a aquellos con la res posibilidad de la supervisión y toma de decisiones.	¿Existe un canal de comunicación interno y externo dentro del gobierno TI?			
		¿Existe supervisión sobre la situación actual de TI respecto a mecanismos de notificación y comunicación?			
	Orientar al personal para que sigue las directrices relevantes para un comportamiento ético y profesional y garantizar que las consecuencias del no cumplimiento se conocen y se respetan.	¿Existe un documento que estipule el reglamento ético y profesional dentro de la organización?			
		¿Conoce usted sobre sanciones que puede recibir si no cumple las reglas o normas de la organización, con el manejo de la gestión IT?			
	Orientar el establecimiento de un sistema de recompensa para promover el cambio cultural deseable.	¿Existe un sistema de recompensas en la empresa por el alcance de un objetivo o metas específicas a cada cargo?			
		¿En caso de poseer un sistema de recompensas, cree que es justo?			
EDM01.03 SUPERVISAR EL SISTEMA DE GOBIERNO Supervisar la ejecución y la efectividad del gobierno de TI de	Evaluar la efectividad y rendimiento de las partes interesadas en las que se he delegado responsabilidades y autoridad para el gobierno de TI de la empresa.	¿Existen métricas de las actividades a realizar en cada cargo?			
		¿Existe un control y seguimiento de las actividades que no se han cumplido?			
	Evaluar periódicamente si los mecanismos para el gobierno de TI	¿Existe una planificación para verificar y controlar el			

Prácticas de gobierno/gestión (Bps)	Actividades	Pregunta para evidenciar el cumplimiento de la actividad	[illegible] cumplen S/N	Comentario	Evidencia
la empresa. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo las estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI.	acordados (estructuras, principios, procesos, etc.) están establecidos y operando efectivamente	funcionamiento de las estructuras, proceso y principios del gobierno IT?			
		¿Existe la documentación de las auditorías internas y externas realizadas a la organización?			
		¿Se han documentado los cambios realizados después de las auditorias?			
	Evaluar la efectividad del diseño del gobierno e identificar las acciones para rectificar cualquier desviación.	¿Posee políticas correctivas en caso de identificar problemas en la gestión IT?			
		¿Existe procesos para controlar desviaciones del gobierno IT?			
	Mantener la supervisión sobre el punto hasta el que TI satisface las obligaciones (regulatorias, legislación, leyes comunes, contractuales), políticas internas estándares y directrices profesionales	¿Se verifica el cumplimiento de las obligaciones de TI, como regulaciones, políticas, etc.?			
		¿Realizan un seguimiento de los requerimientos solicitados por la organización?			
	Proporcionar supervisión de la efectividad de, y el cumplimiento, con el sistema de control de la empresa	¿Existen métricas que puedan calificar la efectividad y cumplimiento del sistema de control de la empresa?			
		¿Existe documentación sobre las métricas utilizadas en la supervisión de la efectividad y cumplimiento del control de la empresa?			
	Supervisar los mecanismos rutinarios y regulares para garantizar	¿Existe supervisión de los mecanismos rutinarios y regulares a realizar en la operación de la empresa?			

Prácticas de gobierno/gestión (Bps)	Actividades	Pregunta para evidenciar el cumplimiento de la actividad	cumplen S/N	Comentario	Evidencia
	que el uso de TI cumple con las obligaciones relevantes (regulatorias, legislación, leyes comunes, contractuales), estándares y directrices				
		¿Se realizan constantes auditorias para ver el cumplimiento de las obligaciones, las mismas que estén acorde a estándares y directrices?			
		¿Existen documentos que evidencien el adecuado cumplimiento de la empresa con respecto a sus obligaciones?			

Tabla 10. Elaboración de las preguntas para la auditoria de cumplimiento
Fuente: Propia

Círculo 2. Aplicar auditoría de cumplimiento a las partes interesadas de la empresa

Una vez establecido los indicadores de atributo para el Nivel 1, como estrategia se conformó un comité de evaluación de procesos en la Universidad Técnica de Machala integrado por los jefes departamentales (partes interesadas) de las siguientes áreas: Tecnología, Talento Humano, Financiero, Compras Públicas, y con el apoyo de las máximas autoridades, para que, de manera consensuada puedan responder a las preguntas planteadas, que bajo la figura de una auditoría de cumplimiento, y sabiendo que como resultado de esta actividad se obtendría la situación actual de los procesos de gobierno y gestión de TI, se cumplió con responsabilidad y conocimiento de causa.

Círculo 3. Establecer mecanismo de valoración – ponderación.

Monica Isabel Bayas Condo (2014), define al término métricas a los indicadores que permiten establecer el porcentaje obtenido del proceso que permitirá encasillarlo en la escala de valoración (N,P,L,F) para establecer el nivel de capacidad del proceso. En este trabajo se ha utilizado como base estos

cálculos, pero se ha realizado unos cambios en las fórmulas, debido a la forma como se establecieron los INDICADORES de ATRIBUTO para nivel 1, estas métricas están en función del número de preguntas elaboradas (NE), de las preguntas cuyas partes interesadas contestaron que sí se cumplía (PC), del peso a cada pregunta (Pe) y finalmente de la sumatoria de las preguntas que sí se cumplen (NSC).

NE	Número total de preguntas planteadas (Tabla 10 Columna 3) para evidenciar el cumplimiento de la actividad y su vez la práctica de gobierno.	
PC	Preguntas cuyo criterio se cumple (Tabla 10 Columna 4 cuya contestación es "S")	
Pe	Peso por cada pregunta	$Pe = \frac{1}{NE}$
NSC	Sumatoria de cuantas preguntas si se cumple	ΣPC
T	Porcentaje para saber la escala de valoración N,P,L,F del proceso	$T = Pe * NSC * 100\%$

Tabla 11. Definición de métricas para determinar la escala de valoración de los procesos
Fuente: Monica Isabel Bayas Condo (2014).

Círculo 4. Establecer escala de valoración para determinar el nivel de capacidad de los procesos.

T	Porcentaje para saber la escala de valoración N,P,L,F del proceso	$T = Pe * NSC * 100\%$

Para definir la escala de valoración, se utiliza las escalas y rangos de la norma ISO/IEC 15504 esto es (N,P,L,F), como ya se describió en las secciones anteriores, esta fórmula se aplica multiplicando el peso de cada pregunta por número de pregunta que sí cumple por 100 para representarla en porcentaje.

Por ejemplo, suponiendo que un proceso tiene la siguiente información:

NE = 39

PC = 15

Pe = 1/39 = 0.026

NSC=15

T = 0.0026 * 15 * 100 = 39%

Nombre del Proceso	**Nivel 0**	**Nivel 1**	**Nivel 2**		**Nivel 3**		**Nivel 4**		**Nivel 5**	
ATRIBUTOS		**PA 1.1**	**PA 2.1**	**PA 2.2**	**PA 3.1**	**PA 3.2**	**PA 4.1**	**PA 4.2**	**PA 5.1**	**PA 5.2**
	100%	**39%**								
Nivel de capacidad alcanzado	**F**	**P**								

N- 0%-15%	P- 15%-50%	L- 50%-85%	F- 85%-100%

Circulo 5, 6, 7, 8.

Una vez establecida la escala de valoración, se verifica si el porcentaje permitió alcanzar la escala "F", si esto es afirmativo se puede seguir analizando los siguientes niveles, en caso contrario se muestra el resultado en el nivel que se está analizando. Para el caso de los niveles 2 hasta el 5 se analiza en base a los indicadores genéricos propuestos por la ISO 15504 preestablecidos (ver Tabla 5).

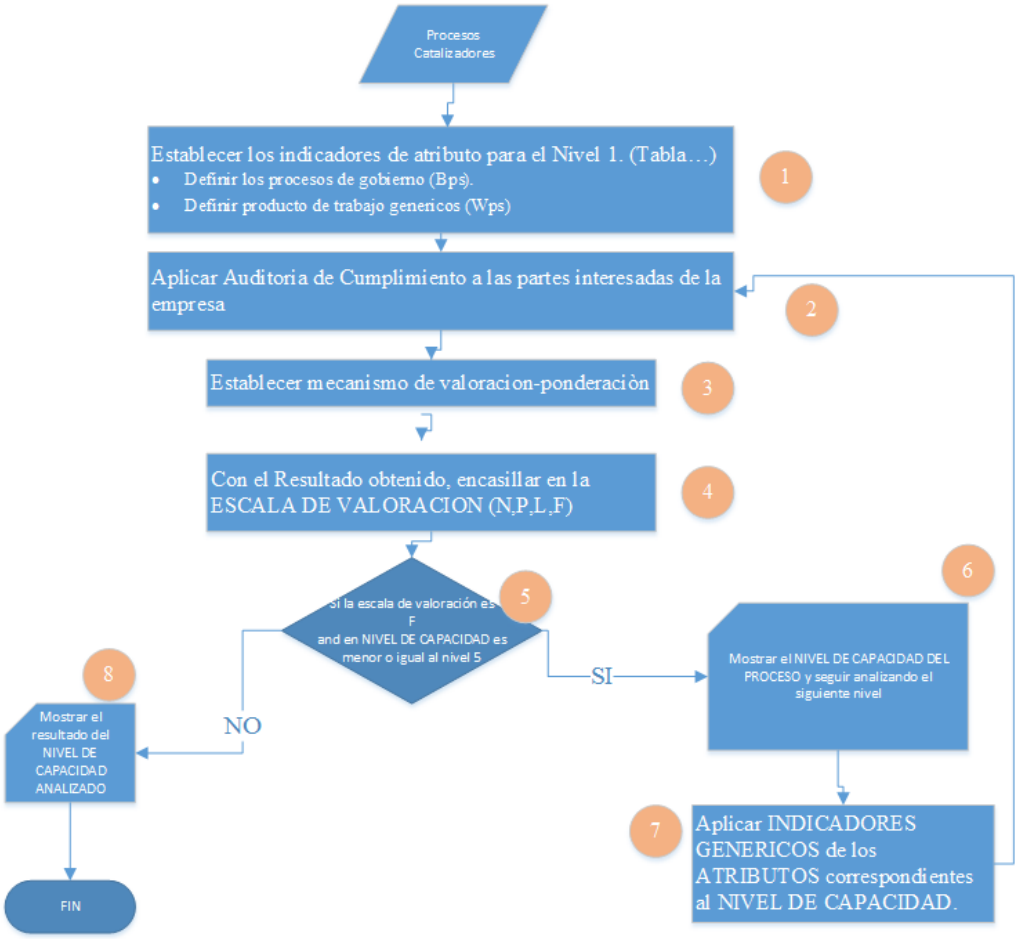


Figura 7.Diagrama de flujo del Modelo de Evaluación de procesos

Fuente: Propio

3.6.2 RESULTADOS OBTENIDOS.

Procesos de COBIT5	NE	PC (Nsc)	Pe	T
EDM01	39	7	0.026	18.2%
EDM02	23	10	0.043	43%
EDM03	19	3	0.053	15.9%
EDM04	15	10	0.067	67%
EDM05	10	1	0.1	10%
APO01	150	50	0.007	35%
APO02	91	43	0.011	47.3%
APO03	80	17	0.013	22.1%

APO04	57	31	0.018	55.8%
APO05	70	13	0.014	18,2%
APO06	66	15	0.015	22,5%
APO07	107	56	0.009	50,4%
APO08	57	38	0.018	68.4%
APO09	52	19	0.019	36.1%
APO10	74	43	0.014	60.2%
APO11	87	42	0.011	46.2%
APO12	29	3	0.034	10,2%
APO13	64	18	0.016	28,8%
BAI01	145	25	0.0069	17,3%
BAI02	23	3	0.043	12,9%
BAI03	89	15	0.011	16,5%
BAI04	90	15	0.011	16.5%
BAI05	85	31	0.012	37.2%
BAI06	51	5	0.020	10%
BAI07	118	2	0.0085	1,7%
BAI08	40	1	0.025	2,5%
BAI09	75	43	0.013	55.9%
BAI10	49	16	0.020	32%
DSS01	114	45	0.009	40.5%
DSS02	27	2	0.037	7.4%
DSS03	20	2	0.05	10%
DSS04	125	33	0.008	26.4%
DSS05	95	51	0.011	56.1%
DSS06	15	2	0.067	13.4%

Tabla 12. Determinación del porcentaje para establecer el nivel de capacidad del proceso
Fuente: Propia

Nombre del Proceso	**Nivel 0**	**Nivel 1**		**Nivel 2**		**Nivel 3**		**Nivel 4**		**Nivel 5**	
ATRIBUTOS		**PA 1.1**		**PA 2.1**	**PA 2.2**	**PA 3.1**	**PA 3.2**	**PA 4.1**	**PA 4.2**	**PA 5.1**	**PA 5.2**
EDM01	**100%**	18,2 %	P								
EDM02	**100%**	43%	P								
EDM03	**100%**	15.9 %	P								
EDM04	**100%**	67%	L								
EDM05	**100%**	10%	N								
APO01	**100%**	35%	P								
APO02	**100%**	47.3 %	P								
APO03	**100%**	22.1 %	P								
APO04	**100%**	55.8 %	L								
APO05	**100%**	18,2 %	P								
APO06	**100%**	22,5 %	P								
APO07	**100%**	50,4 %	L								
APO08	**100%**	68.4 %	L								
APO09	**100%**	36.1	P								

		%					
APO10	**100%**	60.2 %	L				
APO11	**100%**	46.2 %	P				
APO12	**100%**	10,2 %	N				
APO13	**100%**	28,8 %	P				
BAI01	**100%**	17,3 %	P				
BAI02	**100%**	12,9 %	N				
BAI03	**100%**	16,5 %	P				
BAI04	**100%**	16.5 %	P				
BAI05	**100%**	37.2 %	P				
BAI06	**100%**	10%	N				
BAI07	**100%**	1,7%	N				
BAI08	**100%**	2,5%	N				
BAI09	**100%**	55.9 %	L				
BAI10	**100%**	32%	P				
DSS01	**100%**	40.5 %	P				
DSS02	**100%**	7.4%	N				

DSS03	**100%**	10%	N				
DSS04	**100%**	26.4 %	P				
DSS05	**100%**	56.1 %	L				
DSS06	**100%**	13.4 %	N				

Tabla 13. Resultados de los procesos catalizadores con su nivel de capacidad
Fuente: Propia

Debido a que todos los procesos analizados no llegan a la escala de valoración F (completamente alcanzado) en el nivel 1, no se analiza los demás niveles.

Se concluye que la Universidad Técnica de Machala en la actualidad tiene un 29,75% en el nivel 1(EJECUTADO) de cumplimiento de capacidad de los procesos, esto es que los procesos implementados alcanzan su propósito pero no pueden ser medidos (que los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente). El valor de 29,75% es el promedio de los porcentajes obtenidos por cada proceso catalizador como se muestra en la Tabla 13, que en la escala de valoración representa P (Parcialmente alcanzado) esto es, que si hay alguna evidencia de cumplimiento del proceso.

CAPÍTULO IV

4 ESTABLECER PROCESOS PRIORITARIOS MEDIANTE EL MODELO DE CASCADA DE METAS PROPUESTA POR COBIT 5.0 EN LA UNIVERSIDAD TÉCNICA DE MACHALA.

COBIT5.0 plantea 37 procesos para cubrir de extremo a extremo los aspectos de TI en la institución, debido a que la implementación de 37 procesos representa que la institución planifique su presupuesto y tiempo es necesario establecer un mecanismo para priorizar los procesos, de tal manera que se pueda proyectar en el tiempo la implementación de los mismos.

En este sentido, se utiliza cascada de metas de COBIT5.0 cuya metodología se explicó en la Estructura de la Memoria respecto a la descripción del Capítulo IV y se lo representa gráficamente en la Figura 8. Como resumen se puede indicar que el modelo de cascada de metas se convierte en un proceso cuyo insumo son las preocupaciones que escogen las partes interesadas, el resultado del proceso son los procesos prioritarios y las actividades de procesamiento que se deben realizar son las que se muestran en la Figura 8.

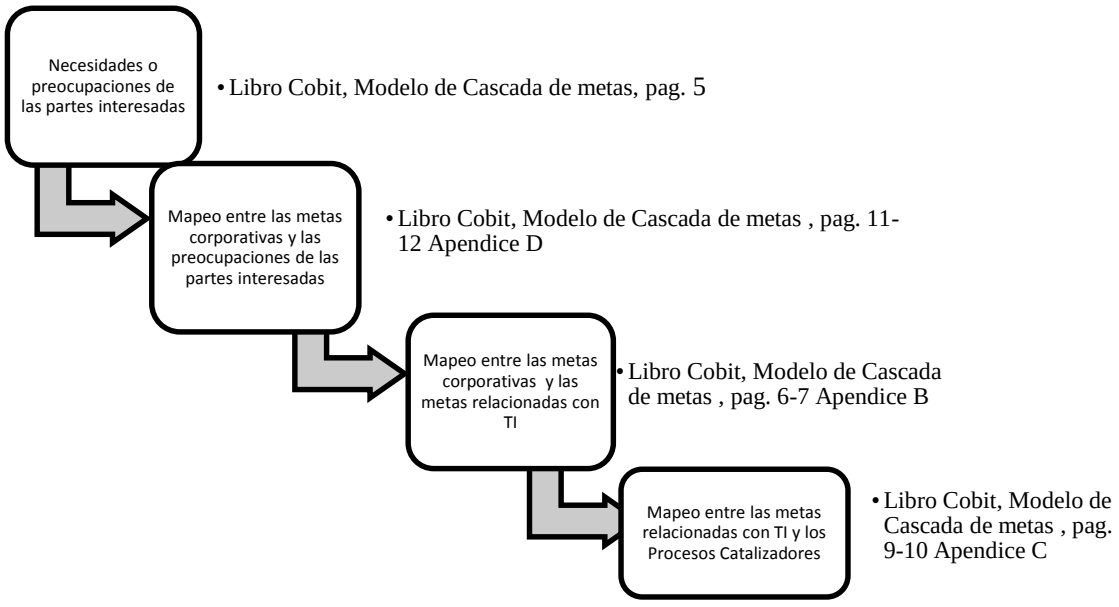


Figura 8. Metodología del Modelo de Cascada de metas

Fuente: Propia

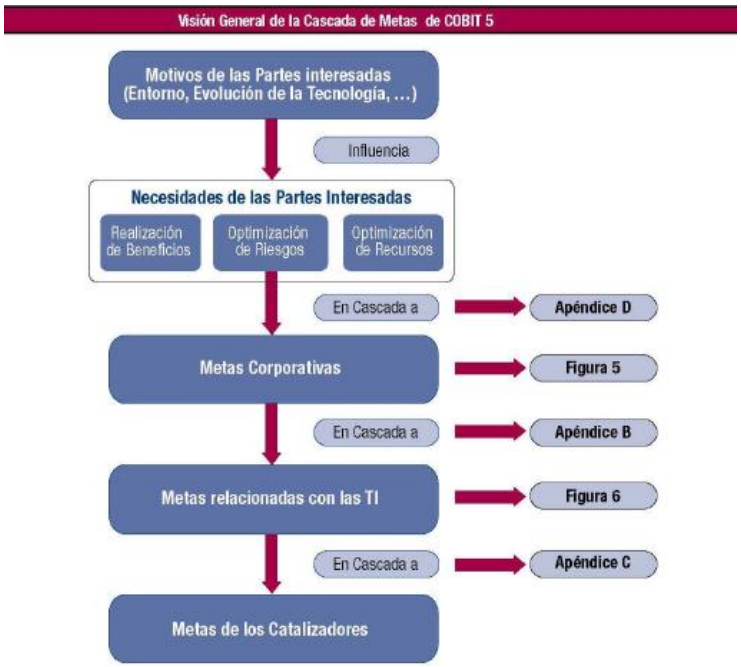


Figura 9. Visión general de Cascada de metas

Fuente: ISACA (2012).

En la Figura 8, se denota cuatro actividades que se deben realizar para el modelo de cascada de metas; la primera actividad "Necesidades o preocupaciones de las partes interesadas", es necesario que la empresa tenga definido correctamente quienes serán las partes interesadas, ellos seleccionaran un número determinado de necesidades, por estrategia se aconseja escoger tres, ya que cada preocupación es probable que genere unos tres procesos catalizadores. En la Tabla 14 se muestra las preocupaciones de las partes interesadas tanto internas como externas establecidas por COBIT 5.0.

Partes Interesadas Internas	Preguntas de las Partes Interesadas Internas
• Consejo de Administración • Director general ejecutivo (CEO) • Director financiero (CFO) • Director de sistemas de información (CIO) • Responsable de riesgos • Ejecutivos del negocio • Propietarios de los procesos del negocio • Responsables del negocio • Responsables de riesgos • Responsables de seguridad • Responsables del servicio • Responsables de recursos humanos • Auditoría interna • Responsables de privacidad • Usuarios de TI • Gerentes de TI • Etc.	• ¿Cómo consigo valor del uso de TI? ¿Están los usuarios finales satisfechos con la calidad del servicio de TI? • ¿Cómo gestiono el rendimiento de TI? • ¿Cómo puedo explotar mejor las nuevas tecnologías para nuevas oportunidades de negocio? • ¿Cómo construyo y estructuro mejor mi departamento de TI? • ¿Cuánto dependo de los proveedores externos? ¿Estoy gestionando bien los contratos de externalización de TI? • ¿Cómo obtengo aseguramiento sobre los proveedores externos? • ¿Cuáles son los requisitos (de control) para la información? • ¿Considero todos los riesgos relativos a TI? • ¿Estoy realizando una operación de TI eficiente y resiliente? • ¿Cómo controlo el coste de TI? ¿Cómo utilizo los recursos de TI de la manera más efectiva y eficiente? • ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes? • ¿Tengo suficiente personal para TI? ¿Cómo puedo desarrollar y mantener sus habilidades y cómo gestiono su rendimiento? • ¿Cómo consigo aseguramiento sobre TI? • ¿Está bien asegurada la información que se está procesando? • ¿Cómo puedo mejorar la capacidad de respuesta del negocio mediante un entorno de TI más flexible? • ¿Fracasan los proyectos de TI en proporcionar lo que habían prometido? Si es así, ¿por qué? ¿Está siendo TI un obstáculo para ejecutar la estrategia de negocio? • ¿Cuán críticas son las TI para la sostenibilidad de la empresa? ¿Qué haría si las TI no estuvieran disponibles? • ¿Qué procesos de negocio críticos dependen de TI y cuáles son los requerimientos de los procesos de negocio? • ¿En cuánto han excedido de media los presupuestos de operación de TI? ¿Con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI? • ¿Qué parte del esfuerzo de TI se dedica a apagar fuegos en lugar de facilitar las mejoras del negocio? • ¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa requeridos? • ¿Cuánto se tarda en la toma de decisiones importantes de TI? • ¿Son transparentes el esfuerzo y las inversiones totales en TI? • ¿Respalda TI a la empresa en el cumplimiento de la normativa y los niveles de servicio? ¿Cómo puedo saber si se cumple con todas las normas aplicables?
Partes Interesadas Externas	**Preguntas de las Partes Interesadas Externas**
• Aliados del negocio • Proveedores • Accionistas • Reguladores/gobierno • Usuarios externos • Clientes • Organizaciones de estandarización • Auditores externos • Consultores • Etc.	• ¿Cómo sé que las operaciones de mi aliado de negocio son seguras y fiables? • ¿Cómo sé que la empresa cumple con las normativas y regulaciones aplicables? • ¿Cómo sé que la empresa está manteniendo un sistema efectivo de control interno? • ¿Los aliados del negocio mantienen bajo control la cadena de información entre ellos?

Tabla 14. Preocupaciones de las partes interesadas internas y externas

Fuente: ISACA, Modelo de Cascada de metas (2012).

La segunda actividad, "Mapeo entre las metas corporativas y las preocupaciones de las partes interesadas", con las preocupaciones seleccionadas de las partes interesadas se establece una relación con las metas corporativas, con la ayuda de la matriz mostrada en la Tabla 15, y como resultado de esta actividad se obtiene las metas corporativas.

Figura 24—Mapeo entre las Metas Corporativas de COBIT 5 y las Preguntas del Gobierno y la Gestión

NECESIDADES DE LAS PARTES INTERESADAS	1. Valor para los interesados de las inversiones de negocio	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio de negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9. Toma estratégica de Decisiones basada en Información	10. Optimización de los costes de los procesos de negocio	11. Optimización de la funcionalidad de los procesos de negocio	12. Programas gestionados de cambio en el negocio	13. Productividad operacional y de los empleados	14. Cumplimento con las políticas internas	15. Cumplimento con políticas internas	16. Personas [competentes y motivadas	17. Cultura de innovación de producto y negocio
¿Cómo se consigue valor mediante el uso de TI? ¿ Está el usuario final satisfecho con la calidad del servicio de TI?	■	■				■	■						■			■	■
¿Cómo se gestiona el rendimiento de TI?		■			■				■	■	■	■		■			
¿Cómo se puede explotar mejor la tecnología de red para conseguir nuevas oportunidades estratégicas?	■	■						■					■			■	■
¿Cómo puedo construir y estructurar mejor mi departamento de TI?								■		■	■	■		■	■	■	
¿Cuánto dependo de mis proveedores externos? ¿Cómo de bien están siendo gestionados los acuerdos de externalización de TI? ¿Cómo puedo verificarlos sobre proveedores externos?			■	■						■							
¿Cuáles son los requisitos (de control) para la información?				■					■						■		
¿He contemplado todo los riesgos relacionados con TI?			■				■		■						■		
¿Estoy ejecutando una operación de TI eficiente y robusta?					■		■										
¿Cómo se controla el coste de TI? ¿Cómo se usan los recursos de TI en la manera más efectiva y eficiente? ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes?										■		■		■			

Tabla 15. Mapeo entre las metas corporativas y las preocupaciones de las partes interesadas

Fuente: ISACA, Modelo de Cascada de metas (2012).

La tercera actividad, "Mapeo entre las metas corporativas y las metas relacionadas con TI", con las metas corporativas obtenidas en la actividad anterior se establece una relación con las metas relacionadas con TI, con la ayuda de la matriz mostrada en la Tabla 16, y como resultado de esta actividad se obtiene las metas relacionadas con TI, como se puede notar en la Tabla 16, la relación se establece con las letras "P" y "S" (Primario y secundario respectivamente), las cuales para establecer valor cuantitativo y definir priorización se le asigna a "P" el valor de 3 por considerarse de mayor prioridad y a "S" el valor de 1.

Figura 22—Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI

		Meta corporativa																
		Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación del producto y del negocio
		1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
	Meta relacionada con las TI	Financiera					Cliente					Interna					Aprendizaje y Crecimiento	
Financiera	01 Alineamiento de TI y la estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	04 Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	06 Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	08 Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
	09 Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P		

Tabla 16. Mapeo entre las metas corporativas y las metas relacionadas con TI

Fuente: ISACA, Modelo de Cascada de metas (2012).

La cuarta actividad, "Mapeo entre las metas relacionadas con TI y los Procesos Catalizadores", con las metas relacionadas de TI de mayor ponderación obtenidas en la actividad anterior se establece una relación con los procesos catalizadores, con la ayuda de la matriz mostrada en la Tabla 17, y como resultado de esta actividad se obtiene los procesos catalizadores, como se puede notar en la Tabla 17, la relación se establece con las letras "P" y "S" (Primario y secundario respectivamente), las cuales para establecer valor cuantitativo y definir priorización se le asigna a "P" el valor de 3 por considerarse de mayor prioridad y a "S" el valor de 1.

Figura 23—Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos *(cont.)*

			Meta relacionada con las TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionan beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Procesos de COBIT 5			Financiera						Cliente		Interna							Aprendizaje y Crecimiento	
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S			P	S	S	S		S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S			S		S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S		
Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio				P			P	S		S				S	S		S

Tabla 17. Mapeo entre las metas relacionadas con TI y los Procesos Catalizadores

Fuente: ISACA, Modelo de Cascada de metas (2012).

a. APLICACIÓN DEL MODELO DE CASCADA DE METAS EN LA UNIVERSIDAD TÉCNICA DE MACHALA.

Actividad 1.

El comité evaluador de procesos definió tres (3) preocupaciones consideradas como importantes, relevantes; estas preocupaciones fueron escogidas de las que plantea COBIT 5.0 ver Tabla 14.

1. ¿Está bien asegurada la información que se está procesando?
2. ¿Cómo consigo aseguramiento sobre TI?
3. ¿He contemplado todos los riesgos relacionados con TI?

Actividad 2.

Mapeo entre las metas Corporativas de COBIT 5 y las preguntas de Gobierno y Gestión.																
NECESIDADES DE LAS PARTES INTERESADAS	**Valor para los interesados de las inversiones de Negocio**	**Cartera de productos y servicios competitivos**	**Riesgos de negocio gestionados (salvaguarda de activos)**	**Cumplimiento de leyes y regulaciones externas**	**Transparencia financiera**	**Cultura de servicio orientada al cliente**	**Continuidad y disponibilidad del servicio de negocio**	**Respuestas agiles a un entorno de negocio cambiante**	**Toma estratégica de decisiones basada en información**	**Optimización de los costes de los procesos de negocio**	**Optimización de la funcionalidad de los procesos de negocio**	**Programas gestionados de cambio en el negocio**	**Productividad operacional y de los empleados**	**Cumplimiento con las políticas internas**	**Cumplimiento con políticas internas**	**Personas preparadas y motivadas**	**Cultura de innovación de producto y negocio**
	1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**	**9.**	**10.**	**11.**	**12.**	**13.**	**14.**	**15.**	**16.**	**17.**
¿Está bien asegurada la información que se está procesando**?**																	

¿Cómo consigo confianza sobre TI?				■											■		
¿He contemplado todos los riesgos relacionados con TI?			■				■		■						■		

Tabla 18. Mapeo entre las metas corporativas de Cobit 5.0 y las preocupaciones de las partes interesadas
Fuente: Propia

Resultado de la actividad 2: Metas Corporativas (cinco).

Riesgos de negocio gestionados (salvaguarda de activos)
Cumplimiento de leyes y regulaciones externas
Continuidad y disponibilidad del servicio de negocio
Toma estratégica de decisiones basada en información
Cumplimiento con políticas internas

Tabla 19. Metas corporativas resultantes
Fuente: Propia

Actividad 3.

Mapeo entre Metas Corporativas de COBIT5 y las Metas Relacionadas con las TI.

		Meta Corporativa					Ponderación					
		Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Continuidad y disponibilidad del servicio de negocio	Toma estratégica de decisiones basada en información	Cumplimiento con políticas internas						
Metas relacionada con las TI		**3**	**4**	**7**	**9**	**15**						
01	Alineamiento de TI y la estrategia de negocio	**S**		S	P		**1**		1	3		**5**

02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	**S**	P			P	**1**	3			3	7
03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	**S**			S		**1**			1		2
04	Riesgos de negocio relacionados con las TI gestionadas	P	S	P		S	3	1	3		1	8
05	Realización de beneficios del portafolio de Inversiones y servicios relacionados con las TI											0
06	Transparencia de los costes, beneficios y riesgos de las TI	S			S		1			1		2

07	Entrega de servicios de TI de acuerdo a los requisitos del negocio	**S**	**S**	S	S		**1**	**1**	1	1		**4**
08	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S		S	S		1		1	1		3
09	Agilidad de las TI	S					1					1
10	Seguridad de la información	P	P	P		P	3	3	3		3	12
11	Optimización de activos, recursos y capacidades de las TI											0
12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en proceso de negocio	S					1					1

13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	**S**					**1**					1
14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	P	**P**		1	1	3	**3**		8
15	Cumplimiento de TI con las políticas internas	S	S			P	1	1			3	5
16	Personal del negocio y de las TI competente y motivado	P					3					3
17	Conocimiento, expectativas e iniciativas para la innovación de negocio				S					1		1

Tabla 20. Mapeo entre metas corporativas y las metas relacionadas con TI
Fuente: ISACA, Modelo de Cascada de metas (2012).

Resultado de la actividad 3: Metas relacionadas con la TI (tres).

Se consideró tomar las metas relacionadas con la TI que tuvieron la mayor ponderación como se muestra en la siguiente tabla.

Metas relacionadas con TI	**Ponderación**
04 Riesgos de negocio relacionados con las TI gestionadas	8
10 Seguridad de la Información	12
14Disponibilidad de información útil y relevante para la toma de decisiones	8

Tabla 21. Metas relacionadas con TI resultantes
Fuente: Propia

Actividad 4.

	Mapeo entre las Metas Relacionadas con las TI de COBIT5 y los Procesos			
	Metas relacionadas a TI			
	04 Riesgos de negocio relacionados con las TI gestionadas	10 Seguridad de la Información	14 Disponibilidad de información útil y relevante para la toma de decisiones	**PONDERACIÓN**
Procesos de COBIT5	**4**	**10**	**14**	

EDM01	**S**	**S**	**S**	1	1	1	**3**
EDM02			**S**			1	**1**
EDM03	P	P	S	3	3	1	**7**
EDM04	S			1			**1**
EDM05			S			1	**1**
APO01	**S**	S	**S**	1	1	1	**3**
APO02	**S**		**S**	1		1	**2**
APO03	**S**	S	**S**	1	1	1	**3**
APO04	S		S	1		1	**2**
APO05	**S**			1			**1**
APO06	S			1			**1**
APO07	**S**	S		1	1		**2**
APO08	**S**			1			**1**
APO09	S	**S**	P	1	1	3	**5**
APO10	P	**S**	S	3	1	1	**5**
APO11	S		S	1		1	**2**
APO12	P	P	S	3	3	1	**7**
APO13	P	P	P	3	3	3	**9**
BAI01	**P**			3			**3**
BAI02	**S**	**S**	**S**	1	1	1	**3**
BAI03	S		S	1		1	**2**
BAI04	S		P	1		3	**4**
BAI05							**0**
BAI06	P	**P**	S	3	3	1	**7**
BAI07	S		S	1		1	**2**
BAI08		S	S		1	1	**2**
BAI09	S	S	S	1	1	1	**3**
BAI10	S	S	P	1	1	3	**5**
DSS01	P	**S**	S	3	1	1	**5**
DSS02	P	**S**	S	3	1	1	**5**
DSS03	P		P	3		3	**6**
DSS04	P	**S**	P	3	1	3	**7**
DSS05	P	P	S	3	3	1	**7**

DSS06	P	**S**	S	3	1	1	**5**
MEA01	P	**S**	S	3	1	1	**5**
MEA02	P	S	S	3	1	1	**5**
MEA03	P	S		3	1		**4**

Tabla 22. Mapeo entre las metas relacionadas con TI y los procesos catalizadores
Fuente: Propia

Resultado de la actividad 4: Procesos Catalizadores prioritarios (seis).

Se consideró tomar las metas relacionadas con la TI que tuvieron la mayor ponderación como se muestra en la siguiente tabla.

Procesos catalizadores prioritarios	Ponderación
APO13 Gestionar la seguridad	9
EDM03 Asegurar la optimización del riesgo	7
APO12 Gestionar el riesgo	7
BAI06 Gestionar los cambios	7
DSS04 Gestionar la continuidad	7
DSS05 Gestionar los servicios de seguridad	7

Tabla 23. Procesos catalizadores prioritarios
Fuente: Propia

CAPÍTULO V

5. PLAN DE ACCIÓN

Este capítulo propone que, luego de establecer seis (6) procesos catalizadores prioritarios como se muestra en la Tabla 23, en base a la ponderación más alta (ver Tabla 22) es necesario establecer los instrumentos necesarios para mejorar el nivel de capacidad de los mismos. El comité evaluador de procesos consideró escoger tres (3) procesos, de estos, para establecer una hoja de ruta o plan de acción de las actividades que deben desarrollarse para la implementación de los mismos y finalmente se propone desarrollar productos entregables como plantillas, procedimientos, controles, manual que permita alcanzar el nivel de capacidad deseado en esos procesos.

Procesos catalizadores prioritarios	**Ponderación**
APO13 Gestionar la seguridad	9
BAI06 Gestionar los cambios	7
DSS05 Gestionar los servicios de seguridad	7

Tabla 24. Procesos catalizadores prioritarios escogidos por el comité
Fuente: Propia

Luego de tener los procesos prioritarios seleccionados, hay que establecer la hoja de ruta de las actividades a desarrollarse para cada proceso que se muestra en la Tabla 24, para lo cual surgen interrogantes, (i) ¿Qué actividades ya están desarrolladas?, (ii) ¿Qué actividades faltan por desarrollar?, (iii) ¿Qué actividades se desarrollarán?.

Para este propósito, se hace uso del diagnóstico de procesos, realizado en el capítulo III (punto 3.2), en el cual se definió el nivel de capacidad de cada proceso catalizador, mediante la aplicación de una auditoria de cumplimiento con la elaboración de un instrumento de investigación basado en la estructura de cada proceso (procesos de gobierno/gestión, entrada, salidas, actividades); en la aplicación del instrumento, el comité que respondió a las interrogantes, definió y

generó la respuesta a la interrogante (i), y por defecto también se define la respuesta a la interrogante (ii), para la interrogante (iii) es necesario establecer una estrategia para resolverla.

Para resolver la interrogante (iii), se utilizó como insumo el nivel de capacidad alcanzado, resultado obtenido luego de que el comité de la UTMACH indicó qué actividades sí cumplían con su respectiva evidencia; con las actividades que falta por cumplir, se estableció reuniones de trabajo con el mismo comité para definir qué actividades son de prioridad (ver Tabla 25) para alcanzar un nivel deseado, ver Tabla 26.

Por nomenclatura, cada actividad seleccionada, se la denomino "hito" ya que estas actividades resultarán muy importantes para mejorar el nivel de capacidad de los procesos, la cual se evidenciará con un producto entregable como se visualiza en la Tabla 25. En esta Tabla se incorpora una columna que muestra la evidencia de cada hito.

PROCESO PRIORITARIO	**HITO**	**ACTIVIDAD PARA ALCANZAR NIVEL DESEADO**	**EVIDENCIA**
BAI06 Gestionar los cambios	Hito 1	¿Posee algún formato de peticiones para atender a los cambios que pueda presentar algún interesado del negocio, ya sea sobre el sistema o aplicaciones, infraestructura o proceso de negocio?	Procedimiento de control de cambios Plantilla de registro de control de cambios Plantilla de registro de tratamiento de cambios
	Hito 2	¿Se lleva un control del proceso de petición de cambios?	
	Hito 3	¿Posee documentación en la que se encuentre categorizado las peticiones de cambio (ejemplo proceso de negocio, infraestructura, sistemas operativos, redes, aplicaciones o sistemas)?	
	Hito 4	¿Se toman a consideración los elementos de configuración afectados en el proceso de categorización de las peticiones de cambios?	
	Hito 5	¿Se supervisa la relación existente entre las peticiones y los elementos de configuración afectados?	

PROCESO PRIORITARIO	HITO	ACTIVIDAD PARA ALCANZAR NIVEL DESEADO	EVIDENCIA
	Hito 6	¿Se tiene priorizados las peticiones de cambio en base a requisitos técnicos y de negocio, recursos y aspectos legales?	
	Hito 7	¿Existe algún documento en la que se encuentren definidas dichas priorizaciones?	
	Hito 8	¿Se supervisa que se cumplan las peticiones de cambio en base a las priorizaciones?	
	Hito 9	¿Posee un plan de contingencia sobre los efectos negativos que puedan causar la implementación de algún cambio?	
	Hito 10	¿Se realiza un análisis de las peticiones de cambios para conocer si existen dependencias entre ellas?	
	Hito 11	¿Se considera en el análisis de las peticiones de cambios aspectos de seguridad, legal y de cumplimientos normativo?	
	Hito 12	¿Se involucra en el análisis de las peticiones de cambios a los jefes departamentales, con la finalidad de socializar dicho análisis?	
	Hito 13	¿Las peticiones de cambio son aprobadas por las personas involucradas en el análisis de dichos cambios (jefes departamentales, gestores de servicios y partes interesadas)?	
	Hito 14	¿Se realiza un Análisis del impacto que causaría los cambios sobre los procesos de negocio, infraestructura, aplicación o sistemas?	
	Hito15	¿Existe algún documento en el que se encuentre evidenciado el punto anterior?	
	Hito 16	¿Existe algún documento en la que se	

PROCESO PRIORITARIO	HITO	ACTIVIDAD PARA ALCANZAR NIVEL DESEADO	EVIDENCIA
		encuentre definido el impacto en los proveedores de servicios contratados en la gestión de cambio?	
	Hito 17	¿Se definen el modo de declarar una petición emergente y con quienes socializar?	
	Hito 18	¿Existe un control acerca de las peticiones de cambios urgentes?	
	Hito 19	¿Existe documentación en la que se defina el plan o procedimientos para afrontar una petición de cambio urgente?	
	Hito 20	¿Se supervisa que los cambios emergentes tengan sean atendidos dando la prioridad del caso?	
	Hito 21	¿Se verifican que los cambios emergentes tengas el acceso de emergencia para ser cumplidos?	
	Hito 22	¿Llevan documentación de las peticiones de cambios emergentes?	
	Hito 23	¿Se supervisa el cumplimiento de todos los cambios de emergencia?	
	Hito 24	¿Se realiza revisiones de la post-implantación de cada uno de los cambios emergentes?	
	Hito 25	¿Se involucran a las partes interesadas en las revisiones de las post-implantaciones?	
	Hito 26	¿Se realiza un control del procedimiento que se emplea para atender un cambio de emergencia?	
	Hito 27	¿Se realiza reuniones con las partes interesadas para analizar, verificar y tomar medidas correctivas sobre el cambio emergente y si impacto sobre el	

PROCESO PRIORITARIO	HITO	ACTIVIDAD PARA ALCANZAR NIVEL DESEADO	EVIDENCIA
		negocio y sus recursos?	
	Hito 28	¿Existe documentación en la que se defina las generalidades de un cambio de emergencia?	
	Hito 29	¿Se socializa con las partes interesadas las generalidades de un cambio de emergencia?	
	Hito 30	¿Las peticiones de cambios se encuentran categorizadas según su estado (rechazados, aprobados no iniciado, aprobados en proceso, cerrado) para realizar su debido proceso de seguimiento?	
	Hito 31	¿Existe algún documento en la que se define las categorías y se encuentren definidos las peticiones según las mismas?	
	Hito 32	¿Se realiza un seguimiento para conocer el estado en el que se encuentra los cambios?	
	Hito 33	¿Se realiza un control de cumplimiento de las peticiones de cambios según los tiempos establecidos?	
	Hito 34	¿Se realiza documentación de los cambios que han sido cerrados o finalizado?	
	Hito 35	¿Se realiza un control de las prioridades que tiene cada uno de los cambios?	
DSS05 Gestionar los Servicios de seguridad.	Hito 36	¿Se definen lineamientos que informen sobre software malicioso a los funcionarios de la organización?	Procedimiento para verificar toda la información relativa a software malicioso.
	Hito 37	¿Se realiza la revisión de manera frecuente sobre información de nuevas posibles amenazas?	

PROCESO PRIORITARIO	HITO	ACTIVIDAD PARA ALCANZAR NIVEL DESEADO	EVIDENCIA
	Hito 38	¿Existe una política de seguridad global referente a conexiones en la organización?	Procedimiento para utilización de los servicios de red
	Hito 39	¿Se define acceso seguro para la conexión de dispositivos en la red de la organización?	Control de acceso a usuarios temporales
	Hito 40	¿Cuáles son los criterios para permitir el acceso a la información de un dispositivo conectado a la red?	Procedimiento para la gestión de medios removibles
	Hito 41	¿Qué nociones se aplican para la definición de contraseñas?	Procedimiento para la administración y custodia de las contraseñas de acceso
	Hito 42	¿Se asegura la información mediante el proceso de cifrado de la misma en función a categorías pre establecidas?	
	Hito 43	¿Se bloquean los equipos durante horas no laborables en la organización?	Restringir el tiempo de conexión de los usuarios considerando las necesidades de la institución
	Hito 44	¿Se posee directrices para gestionar el acceso remoto a los equipos de cómputo de la organización?	Procedimiento para gestión de equipos de acceso remoto
	Hito 45	¿Existe un documento que da contexto del procedimiento de dar de baja un equipo de cómputo de un usuario final?	Control de acceso a usuarios temporales
	Hito 46	¿Se determinan solicitudes para realizar un cambio de equipo a un usuario final?	
	Hito 47	¿Se considera la contaminación que puede producir el deshacerse de los equipos de cómputo?	Procedimiento de los medios de respaldo, una vez concluida su vida útil recomendada por el proveedor y la destrucción de estos medios
	Hito 48	¿Se aplican normativas para la autentificación fundamentada en una clasificación adecuada bien definida en cuanto al acceso de información?	Procedimiento para que la información sensible sea protegida durante la recolección, procesamiento y almacenamiento

PROCESO PRIORITARIO	HITO	ACTIVIDAD PARA ALCANZAR NIVEL DESEADO	EVIDENCIA
	Hito 49	¿Se administra la autenticación de manera correcta?	Procedimiento de registro de inicio seguro
	Hito 50	¿Se capacita al personal sobre los dispositivos de seguridad tecnológicos que se emplean en las ubicaciones TI sensibles?	Procedimiento para la administración de medios informáticos de almacenamiento
	Hito 51	¿Se gestiona la recepción, uso, eliminación y destrucción de formularios fundamentados en normativas predefinidas?	Procedimiento para la gestión de medios removibles
	Hito 52	¿Las operaciones de gestión de los dispositivos de salida se controlan tanto como dentro, así como fuera de la empresa?	
	Hito 53	¿Se controla la presencia de incidentes de manera frecuente en los registros de eventos?	Procedimiento para administrar los incidentes de seguridad de la información
	Hito 54	¿Se implementa sistemas en línea para la recopilación de evidencias de procesos forenses locales?	Ficha para registrar el tratamiento de incidentes
	Hito 55	¿Se notifica a todos los funcionarios eficientemente sobre evidencias de procesos forenses realizados en la organización?	
APO13 Gestionar la seguridad	Hito 56	¿Define una metodología de evaluación de riesgos apropiada para el SGSI?	Manual para evaluación de riesgos
	Hito 57	¿Establece criterios de aceptación de riesgos y sus correspondientes niveles?	

PROCESO PRIORITARIO	HITO	ACTIVIDAD PARA ALCANZAR NIVEL DESEADO	EVIDENCIA
	Hito 58	¿Define los requerimientos de seguridad de activos de información para así determinar el plan de riesgo	
	Hito 59	¿El plan de tratamiento de riesgo formulado, detalla los controles seleccionados para la mitigación de riesgos encontrados?	
	Hito 60	¿Dispone de un listado de las principales amenazas comunes que existen en la organización permitiendo así la detección temprana de eventos de seguridad	

Tabla 25. Procesos catalizadores prioritarios con los hitos para alcanzar nivel deseado
Fuente: Propia

Con los hitos planteados en la Tabla 25, se alcanza en el nivel 1 de capacidades un considerable avance en la escala de valoración, obteniendo la escala "L" (Ampliamente alcanzado) con evidencias de un enfoque sistemático y de un logro significativo del atributo definido en el proceso evaluado. Pueden encontrarse algunas debilidades relacionadas con el atributo en el proceso evaluado con un rango entre 50 a 85 por ciento de logro. Los resultados que se esperan se muestran en la Tabla 26.

Para calcular el valor que se muestra en la columna 4 de la Tabla 22 "Puntuación deseada", se consideró tomar como ejemplo el proceso APO13, esto es el valor 8% se aplicó de la siguiente manera:

a) Se tomó los datos de la Tabla 12 para cada proceso

Procesos de COBIT5	NE	PC (Nsc)	Pe	T
APO13	64	18	0.016	28,8%

b) Se aplicó las fórmulas que se detalló en el Capítulo 3 y permitió obtener los valores de la Tabla 13.

c) Los cálculos fueron los siguientes.

En la tabla 21 se denota que para el proceso APO13 se agregaran 5 actividades o hitos por lo tanto el cálculo se lo hace con este valor

Pe=0.016*5*100 = 8%

Proceso	Puntuación alcanzada	Nivel de capacidad alcanzado	Puntuación deseada	Nivel de capacidad deseada
APO13 Gestionar la Seguridad	28,8%	Nivel 1 Ejecutado P. Parcialmente alcanzado	28,8%%+ 8% Total=36,8%	Nivel 1 P. Parcialmente alcanzado
BAI06 Gestionar los cambios	10%	Nivel 1 Ejecutado N. No alcanzado	10% + 68,6% Total= 78,6%	Nivel 1 Ejecutado L. Ampliamente alcanzado
DSS05 Gestionar los servicios de seguridad	56,1%	Nivel 1 Ejecutado L. Ampliamente alcanzado	56,1% + 21,05% Total= 77,15%	Nivel 1 Ejecutado L. Ampliamente alcanzado

Tabla 26. Procesos catalizadores prioritarios con los hitos para alcanzar nivel deseado
Fuente: Propia

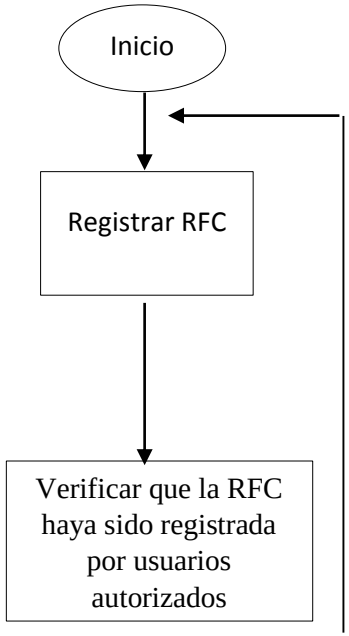
Para cada uno de los hitos planteados en la Tabla 25, se establece la evidencia (plantillas, procedimiento, controles, manual); que luego con el impulso del rectorado como máxima autoridad, se implemente, para mejorar el nivel de capacidad de los procesos prioritarios. En este sentido, como aporte del trabajo, se plantea los siguientes instrumentos:

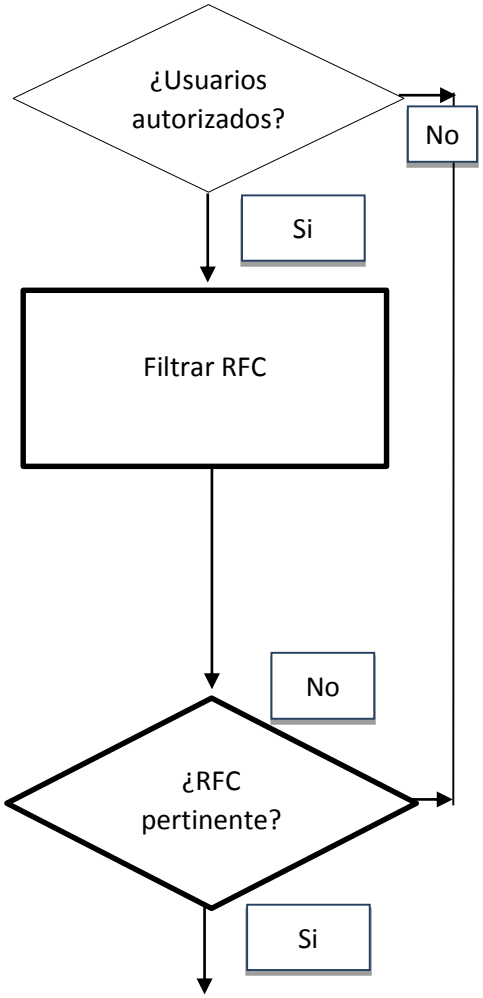
PROCESO BAI06 GESTIONAR LOS CAMBIOS HITO 1 AL 35

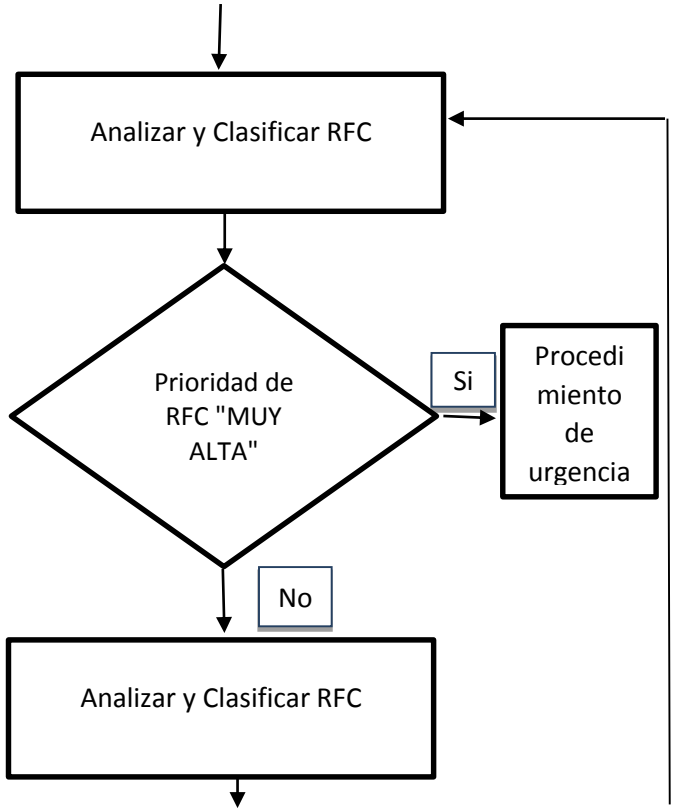
	PROCEDIMIENTO DE CONTROL DE CAMBIOS			Código: PR-GTI- Revisión: Rev-0 Fecha:
Elaborado por:	Dirección Tecnologías de la Información	Revisado por: Director de TI	Aprobado por: Director de TI	p. 1 de 1
1. Propósito:	Establecer las directrices para regular los cambios.			
2. Alcance:	Aplica a los cambios en el software, aplicaciones, sitios web y bases de datos residentes en el centro de procesamiento de datos			
3. Responsabilidad y Autoridad				
Función	Responsabilidad		Autoridad	
3.1 Usuario autorizado	Elaborar la solicitud de cambio y dirigirla al Oficial de seguridad de la Información			
3.2 Oficial de Seguridad de la Información	Verifica el cumplimiento del procedimiento			
3.3 Consejo asesor de cambios	Conformado por: Representante de la alta dirección, Director de TI, Representante de Proveedores de S/W, Oficial de seguridad de la información, Encargado de: Filtrar, analizar y clasificar la RFC			
3.4. Director de TI	Aprobar las tareas de implementación del cambio, monitorear y mantener registros del proceso de implementación del cambio (manuales de usuario, versiones de las aplicaciones, pruebas), abrir ventanas de mantenimiento			
3.5 Implementadores del cambio	Realizar las tareas de desarrollo, pruebas y puesta en marcha de los cambio, cumplir con lo estipulado en la implementación del cambio			

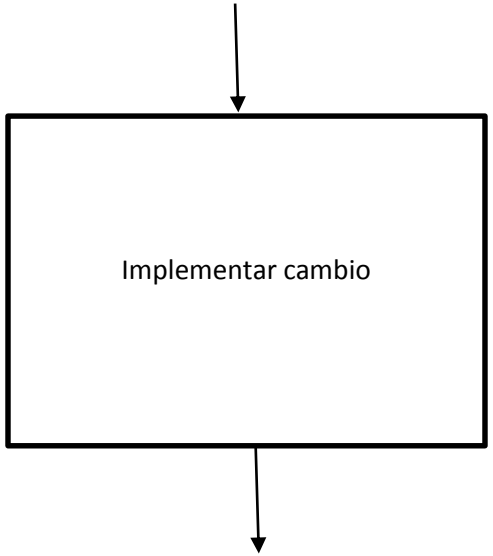
4. Definiciones	
RFC	REQUEST FOR CHANGE - DOCUMENTO DE SOLICITUD DE CAMBIO

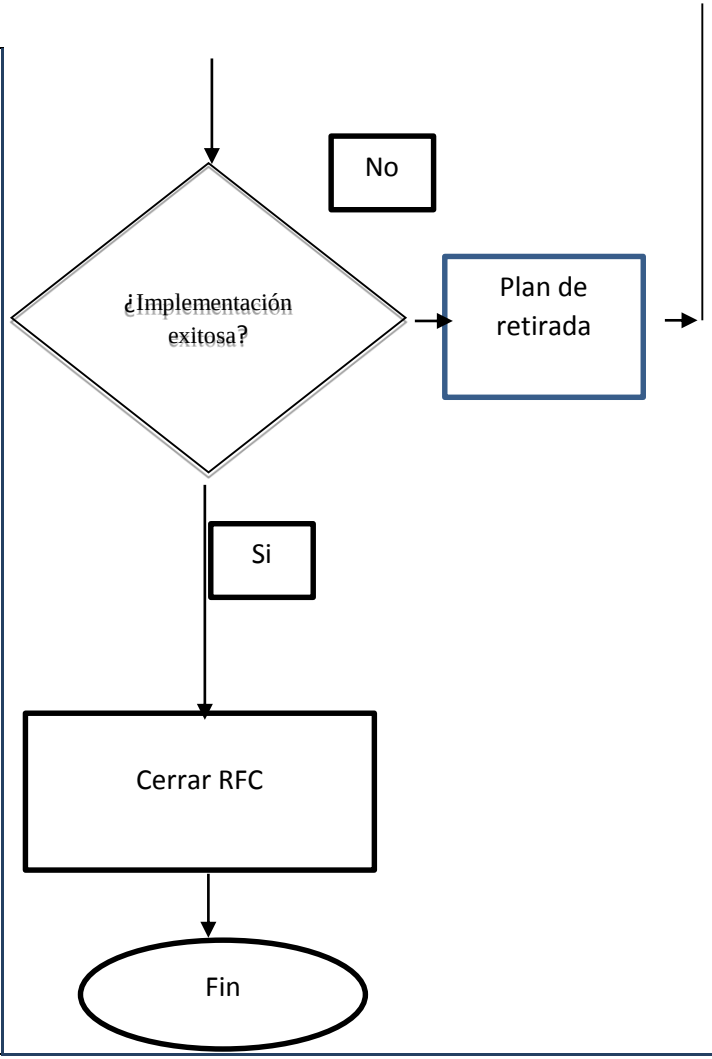
5. Descripción

Responsable	Actividades	Detalle	Registros
			
a) Usuario autorizado		La alta dirección puede solicitar cambios como resultado de una redirección estratégica o cambios en la legislación, los proveedores pueden introducir importantes mejoras a sus productos, las gerencias departamentales pueden proponer soluciones a errores conocidos o desarrollo de nuevos servicios.	Registro de Solicitud de Cambios
b) Consejo asesor de cambios o Dirección de tecnología de la información		El Consejo Asesor de Cambios de la información verificará que la RFC ha sido registrada por usuarios autorizados	Registro de solicitud de cambios

c) Consejo asesor de cambios		
	Evalúa preliminarmente su pertinencia. Una RFC puede ser simplemente no válida si se considera que el cambio no está justificado o se puede solicitar su modificación si se considera que algunos aspectos de la misma son susceptibles de mejora o mayor definición. En cualquiera de los casos la RFC debe ser devuelta a quien lo solicitó con el objetivo de que se puedan realizar nuevas alegaciones a favor de dicha RFC o para que pueda ser consecuentemente modificada.	Registro de solicitud de cambios

d) Consejo asesor de cambios			
		Analiza la prioridad del cambio solicitado "MUY ALTA", "ALTA", "MEDIA" o "BAJA", puede entonces ratificarla o cambiarla de forma tal que se pueda determinar los recursos según cada caso.	Registro de tratamiento de cambios
		Un procedimiento de urgencia supone destinar todos los recursos necesarios para implementar los cambios lo más rápidamente posible.	
e) Gestión de tecnología		Definen los recursos necesarios para el proceso de cambio, cronogramas de actividades a realizar, respaldos previos, conjunto de pruebas pre y post implementación, capacitación de usuarios, plan de back out/vuelta atrás,	

f) Gerencia de Sistemas, Implementadores del cambio y Oficial de Seguridad de la Inf.		Monitorizan el proceso de implementación para asegurar que: - Los cambios al software se ajustan a las especificaciones predeterminadas. - Se cumplen los calendarios previstos y la asignación de recursos es la adecuada. - Se obtenga la aprobación del responsable de sistemas para las tareas a desarrollar. - Se obtenga la aprobación del Oficial de Seguridad de la Inf para garantizar la seguridad de los datos. - El entorno de pruebas es realista y simula adecuadamente el entorno de producción. -Se mantenga un control de versiones para las actualizaciones del software - Los planes de "back-out/vuelta atrás" permitirán la rápida recuperación de la última configuración estable. - Se permita el acceso controlado de usuarios al entorno de pruebas para que realicen una valoración preliminar de los nuevos sistemas en lo que respecta a su: Funcionalidad. Usabilidad. Accesibilidad.	(Registro de tratamiento de cambios)

g) Usuario autorizado		Solicita la ejecución del plan de vuelta atrás/retorno es decir el uso de la última versión del software estable	
h) Consejo asesor de cambios		Evalúa la implementación del cambio para mejora continua	Registro de tratamiento de cambios)

6. Control de Registros						
Identificación	Tipo	Responsable de recolección	Tiempo Retenc.	Recuperación y acceso	Almacenamiento y Protección	Disposición final
Elaborado:						*Machala, Julio /2017*

Plantilla de REGISTRO DE CONTROL DE CAMBIOS

ID Cambios		Estado:	Aprobado	☐
Fecha y hora del cambio				
Nombre del Funcionario				
Departamento				
Descripción del cambio solicitado				
Motivo				
Beneficios esperados				

PLANTILLA DE REGISTRO DE TRATAMIENTO DE CAMBIOS

ID Cambios		Estado:	Registrado	☐
Fecha y hora del tratamiento		Hito 30	En ejecución	☐
Nombre del Funcionario			Suspendido	☐
Departamento			Resuelto	☐
			Cerrado	☐

CLASIFICACIÓN DEL INCIDENTE		
Tipo de servicio afectado Hito 3	Nivel de severidad Hito6	
EJM: Red, Internet, Datos, DB Oracle, Oracle Web Logic,	Impacto del cambio	Impacto en el Tiempo
Pagina Web, Biometricos, FO, utp, switch,	Alto ☐	
Pérdida del servicio de red del equipo o de las prestaciones,	Medio ☐	
Mal funcionamiento del software o del hardware, etc.	Bajo ☐	
Nivel de autorización para la Implantación del cambio:		

Llenar sólo en el caso de que se produjeran varios eventos simultáneos

Urgencia o prioridad de atención del incidente	Alto ☐	Medio ☐	Bajo ☐

Listar las tareas a realizar		
Fecha	Tarea	Responsable
Tareas a realizar en el ambiente de pruebas		
Estradas	Tarea	Resultados Esperados

Solicitud de autorización al propietario de la información		
Fecha	Descripción	Firma
Notificación a usuarios		
Fecha	Usuario notificado	Firma

Solicitud de acceso remoto			
fecha	hora inicio	hora fin	Acciones de cambio, pruebas y configuración

Impacto sobre la aplicación informática

Mucho impacto al software base (Hito 7)

Si ☐	No ☐
Si la respuesta es Si, detallar un plan de contingencia , posibles riesgos Hito 9	

_____

Personal de Tecnología
Encargado del Incidente

_____

Responsable de
Seguridad
de la Información

Copia a: Director Tecnología de la Información
Oficial de Seguridad de la Información

HITO 36 y 37. PROCEDIMIENTO PARA VERIFICAR TODA LA INFORMACIÓN RELATIVA A SOFTWARE MALICIOSO.

PROPÓSITO.

Establecer acuerdos o convenios con empresas que publiquen novedades, boletines informativos de los nuevos sucesos respecto a la seguridad de la información, información que permita socializarla, comunicarla a todo el personal de la UTMACH con el objetivo de prevenir sobre riesgos informáticos.

ALCANCE.

Todos los usuarios de UTMACH, y entidades externas que formen parte del contexto de la institución, con vinculación de intercambio de información con UTMACH.

PROCEDIMIENTO.

1. El Director de Tecnología selecciona la o las empresas que publiquen información relevante, actual sobre temáticas de seguridad de la información.
2. El Oficial de la Seguridad de la información genera los convenios para recibir información actualizada, por algún medio de intercambio con las políticas de seguridad ya establecidas.
3. El Responsable de seguridad de la Dirección de Tecnología de la Información evalúa la información que es importante socializarla con los usuarios a través de una cartelera pública.
4. Si la información es considerada como importante para prevenir riesgos de la información, el responsable de seguridad de la Dirección de Tecnología debería comunicarla o difundirla.
5. El Responsable de seguridad de la Dirección de Tecnología de la Información tiene como responsabilidad mantener la cartelera de seguridad de la información actualizada.

HITO 38. PROCEDIMIENTO PARA UTILIZACIÓN DE LOS SERVICIOS DE RED

PROPÓSITO.

Impedir el acceso no autorizado a los servicios en red mediante políticas para el control de acceso a la información, a las instalaciones de procesamiento de la información, los cuales deberán ser controlados sobre la base de los requisitos y seguridad.

ALCANCE.

Esta política se aplica a todos los funcionarios, servidores públicos a honorarios y terceras partes que tengan derechos de acceso a la información que puedan afectar los activos de información que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Responsabilidades de la Administración de la Dirección de Tecnología:

- El responsable encargado o la Unidad TI será responsable de mantener la operatividad del servidor donde se aloje el servicio y atenderá las fallas que el mismo presente tanto a nivel del sistema operativo como a nivel de hardware.
- La creación de cuentas asignadas a miembros de la institucion que no sean personal regular dentro de la Nómina Central de RRHH, debe asignarse con una vigencia controlada.
- Las cuentas asignadas a los miembros de la institución autorizados deberán ser eliminadas en caso de que la misma no haya sido utilizada sin ningún tipo de notificación; o por requerimiento de su supervisor inmediato siguiendo los procedimientos establecidos para tal fin.
- La asignación de las cuentas se realizará a través de su jefe superior
- Los acuerdos o compromisos asociados al servicio deberán estar definidos y ser respetados para dar cumplimiento a la prestación del mismo de forma oportuna y correcta.
- En el servicio ofrecido por la institución no se podrá enviar correos con archivos anexos que tengan las extensiones ad, scr, mp3, mp4, pif, exe, bat, cmd, com, B64, mim, BHX, Uu, hqx, pIF, HQX, porque son susceptibles a la transmisión de virus y software malicioso.

- El responsable encargado de la implementacion de servicios deberá notificar a través del correo interno a los usuarios de la suspensión del servicio por razones de mantenimiento o por fallas ocurridas en la operatividad del mismo.

PROCEDIMIENTO.

1. El personal responsable de la Dirección de Tecnología con funciones para administrar la red debe tener un listado de servicios de red activos para los funcionarios de UTMACH autorizados.
2. El personal responsable de la Dirección de Tecnología con funciones de la administración de la red debe establecer reuniones de trabajo con cada jefe departamental para autorizar a cada funcionario el acceso al servicio de red.
3. Si un personal temporal, o por cambio de funciones, o personal nuevo en sus funciones, el jefe departamental deberá solicitar a la Dirección de Tecnología con copia al Oficial de Seguridad el acceso a los respectivos servicios de red.
4. El administrador de la red deberá controlar el acceso a los servicios de red tanto internos como externos.
5. El administrador de la red identificará las redes y servicios de red a los cuales se permite el acceso.
6. El administrador de la red debe realizar normas y procedimientos de autorización de acceso entre redes.
7. Establecer controles y procedimientos de administración para proteger el acceso y servicios de red.
8. El administrador de la red deberá identificar los equipos conectados a la red.
9. Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, Servidores y equipos de usuario final, estarán habilitados sólo para los administradores de red.
10. Los usuarios finales deberán permitir tomar el control remoto de sus equipos por el Área de Soporte, teniendo en cuenta, no tener archivos con información sensible a la vista, no desatender el equipo mientras se tenga el control del equipo por un tercero.
11. Los puertos, servicios y medios similares instalados en una computadora o red, que no son requeridos específicamente por funcionalidad, serán desactivados o removidos.

12. El administrador de red deberá generar grupos de servicios de información, usuarios y sistemas de información para segregarlos en redes, es decir, divididas en redes de comunicación más pequeña para mejorar no sólo la seguridad, sino también el rendimiento.
13. La segregación de las redes se basará en el valor y la clasificación de la información almacenada o procesada en la red, niveles de confianza o líneas comerciales; para así reducir el impacto total de una interrupción del servicio.

HITO 39. CONTROL DE ACCESO A USUARIOS TEMPORALES

Cada jefe departamental debe solicitar el usuario temporal a quien debe autorizar y crear contraseña. El registro de solicitud debe tener la siguiente información: Usuario, tiempo de vigencia de acceso, hora y fecha de inicio, hora y fecha de finalización, recursos a los que debe acceder.

La Dirección de tecnología debe evaluar la solicitud, autorizar en caso de ser necesario, estar pendiente de revocar la autorización cuando se cumpla la hora y fecha de finalización.

HITO 40,51,52 PROCEDIMIENTO PARA LA GESTIÓN DE MEDIOS REMOVIBLES

PROPÓSITO.

Definir las reglas para la protección de los datos en diferentes medios de almacenamiento y evitar la divulgación no autorizada, modificación, borrado o destrucción de los activos e interrupción de las actividades de negocio.

ALCANCE.

Se aplica a todos los usuarios de UTMACH, ya sean funcionarios, contratados, practicantes, consultores, incluyendo las empresas que presten servicios en UTMACH.

Aplica a todos los medios de almacenamiento removibles como son: Discos externos, pendrive, Cd y DVD, que hayan sido entregados por la UTMACH a los usuarios.

ROLES Y RESPONSABILIDADES.

- **Jefe Departamental.** Solicitar la asignación de medios removibles para personal de su dependencia.
- **Director de tecnología.** Evaluar y autorizar su uso.
- **Usuario.** debe mantener el debido resguardo de la información contenida en el medio removible que le fue asignado. Informar de manera oportuna de cualquier deterioro. Ocuparse de su uso, ubicación, análisis de virus, eliminación de datos en forma segura cuando corresponda.
- **Personal de la Dirección de Tecnología.** Configurar a los PC no autorizados para denegar acceso a los medios removibles.

DESARROLLO.

1. Los usuarios no pueden utilizar un medio removible no autorizado y que no haya sido dado por la UTMACH.
2. Los usuarios solicitarán una ubicación con seguridad para el dispositivo.
3. Los jefes departamentales solicitarán al Director de Tecnología la asignación de dispositivos indicando los motivos y qué tipo de información se usará en el almacenamiento.
4. Los usuarios tienen que escanear mediante antivirus cada vez que sea conectado a un equipo de UTMACH.
5. El Director de tecnología en la entrega del dispositivo debe registrar el tiempo de vida útil para considerar su destrucción y eliminación correcta de la información.
6. La información almacenada en medios removibles que requiera estar disponible después del tiempo de vida del medio, debe ser almacenado en cualquier otro medio de manera de garantizar que no exista pérdida de información.
7. Toda vez que se requiera almacenar y transportar información sensible en medios removibles debe ser mediante herramientas de cifrado.
8. Cuando la información almacenada en un medio removible pierda vigencia, se debe formatear o destruir el medio en forma segura.

9. El personal de la Dirección de Tecnología debe monitorear el buen uso de los dispositivos y en cumplimiento con la información antes detallada.
10. Los jefes departamentales en conjunto con el Director de tecnología deberán analizar la pertinencia de restringir el acceso a los puestos USB, mediante configuración a nivel de software.

HITO 41 Y 42. PROCEDIMIENTO PARA LA ADMINISTRACIÓN Y CUSTODIA DE LAS CONTRASEÑAS DE ACCESO.

PROPÓSITO.

Las contraseñas son un aspecto fundamental de la seguridad de los recursos informáticos. Es la primera línea de protección para el usuario. Una contraseña mal elegida o protegida puede resultar en un agujero de seguridad para toda la organización. Por ello, todos los usuarios de UTMACH son responsables de velar por la seguridad de las contraseñas seleccionadas por ellos mismos para el uso de los distintos servicios ofrecidos por UTMACH.

Es importante la protección de dichas contraseñas, y el cambio frecuente de las mismas.

DESARROLLO.

Todas las contraseñas de cuentas que den acceso a recursos y servicios de UTMACH deben ser cambiados al menos una vez cada seis meses, se recomienda cambiarla con mayor frecuencia y también siempre que el usuario sospeche que la seguridad de su contraseña pueda haber sido comprometida.

Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas.

En la medida de lo posible, las contraseñas serán generadas automáticamente con las características recomendadas en esta política y se les comunicará a los usuarios su

contraseña siempre en estado “expirado” para obligar al usuario a cambiarla en el primer uso que hagan de la cuenta o servicio.

SELECCIÓN Y CUSTODIA DE CONTRASEÑAS.

Las contraseñas son usadas con múltiples propósitos en UTMACH, como pueden ser las contraseñas de cuentas de usuario, servicios Web, cuentas de correo electrónico, protectores de pantalla en los recursos de los usuarios, administración de dispositivos remotos, etc. Se debe poner especial atención en la selección de contraseñas seguras para la autentificación en todos los recursos y servicios de UTMACH.

La seguridad de este tipo de autentificación se basa en dos premisas:

1. La contraseña personal sólo la conoce el usuario.
2. La contraseña es lo suficientemente “fuerte” para no ser descifrada.

Las contraseñas no deben ser almacenadas por escrito nunca.

Los usuarios deben custodiar las claves en archivos encriptados, si lo hacen en pendrive tiene que estar ubicado bajo llaves.

RECOMENDACIONES PARA LA PROTECCIÓN DE LA CONTRASEÑA.

- No revele su contraseña por teléfono a NADIE, incluso aunque le hablen en nombre del servicio de informática o de un superior suyo en la organización.
- No revele la contraseña en mensajes de correo electrónico ni a través de cualquier otro medio de comunicación electrónica.
- Nunca escriba la contraseña en papel y lo guarde. Tampoco almacene contraseñas en ficheros de ordenador sin encriptar o proveerlo de algún mecanismo de seguridad.
- No revele su contraseña a sus superiores, ni a sus colaboradores.
- No hable sobre una contraseña delante de otras personas.
- No revele su contraseña en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo.
- No comparta la contraseña con familiares.
- No revele la contraseña a sus compañeros cuando se marche de vacaciones.

- No utilice la característica de "Recordar Contraseña" existente en algunas aplicaciones
- (Outlook, Netscape, Internet Explorer).
- Si sospecha que una cuenta o su contraseña pueden haber sido comprometidas, comuníquelo al responsable de la seguridad de la información y cambie las contraseñas de todas sus cuentas.
- Cambie las contraseñas con la frecuencia recomendada para cada tipo de cuenta y servicio.

ESTÁNDARES DE DESARROLLO DE APLICACIONES

Los desarrolladores de aplicaciones informáticas para UTMACH y que gestionen sus propios mecanismos de autentificación mediante contraseñas, deben asegurarse de que sus programas contienen las siguientes precauciones en términos de seguridad respecto de la selección y uso de contraseñas:
Deben proveer de un mecanismo para expirar las contraseñas y obligar a los usuarios al cambio de la misma.
Se debe limitar el número de intentos de accesos sin éxito consecutivos.

HITO 43 CONTROLES PARA RESTRINGIR EL TIEMPO DE CONEXIÓN DE LOS USUARIOS CONSIDERANDO LAS NECESIDADES DE LA INSTITUCIÓN.

El jefe departamental deberá informar al Oficial de Seguridad de la Información la petición de restringir el acceso a ciertas horas y este solicitar a la Dirección de tecnologías que se proceda a aplicar la restricción.

Los jefes departamentales tendrán la responsabilidad de analizar si a un usuario autorizado deba restringirle el acceso a ciertas horas que pueda ser el horario de trabajo autorizado, pueda ser restringir el acceso a días laborables y no sábado y domingo. En caso necesario de que un usuario deba acceder fuera del horario establecido deba pedir autorización a su jefe departamental.

HITO 44. PROCEDIMIENTO PARA GESTIÓN DE EQUIPOS DE ACCESO REMOTO.

PROPÓSITO

El Propósito de este documento normativo es establecer las normas y procedimientos que deberán seguirse para la seguridad en el servicio de acceso remoto. Se busca con esto proteger la información electrónica de UTMACH, la cual puede resultar inadvertidamente comprometida por los riesgos que implican las conexiones remotas a sus sistemas de información.

ALCANCE

Aplican a todo usuario autorizado por la UTMACH para operar una computadora con capacidad de acceso remoto.

DEFINICIONES.

- **Usuario autorizado.** Personal de UTMACH que tiene una cuenta en la red con el propósito de ejercer funciones laborales con autorización de acceso remoto. Personal externo a la UTMACH que requiere acceso remoto como parte de un servicio que provee a la UTMACH.
- **VPN:** Red virtual privada que proporciona un medio para aprovechar un canal público como la Internet, para tener un canal privado o propio, que permita comunicar datos privados. Esto se logra con un método de codificación y un túnel seguro, que cree una vía privada y segura a través de la Internet.
- **Firewall:** sistema o grupo de sistemas que establece una política común de seguridad para red privada y la Internet, determinando a qué servicios de la red pueden acceder los usuarios internos y externos.

DESARROLLO.

1. Toda persona que requiera conectarse remotamente a algún sistema de información deberá llenar la solicitud de acceso remoto para su debida autorización.

2. Un usuario, a quien se le conceda el privilegio de acceso remoto, deberá estar consciente tanto de que la conexión entre su localidad y la UTMACH son extensiones a la red de la UTMACH como de la responsabilidad que esto conlleva.
3. Toda conexión remota debe coordinarse con la Dirección de Tecnologías.
4. El acceso remoto debe realizarlo con una herramienta tecnológica que permita realizar trazabilidades (logs para realizar auditoria), con tecnología de encriptación de datos.
5. Todo permiso otorgado a conexión remota deberá eliminarse una vez finalice el trabajo autorizado.

RESPONSABILIDADES

Director de tecnología:

- De gestionar y mantener los recursos tecnológicos que se necesiten para la UTMACH pueda proveer los servicios de acceso remoto, basados en el servicio necesario o trabajo a realizarse, a los usuarios autorizados
- Ofrecer apoyo a las diferentes áreas que puedan requerir una conexión remota para que la misma pueda establecerse adecuadamente y de acuerdo con las normas de seguridad establecidas.
- Recibir, evaluar y procesar las solicitudes de acceso remoto.
- Hacer conocer el procedimiento aquí establecido al personal que pueda requerir conectarse al acceso remoto.
- Los jefes departamentales tendrán la responsabilidad de solicitar acceso remoto, utilizando las formas de solicitud de acceso remoto.

Administrador de la Red:

- Configurar adecuadamente el firewall o cualquier herramienta tecnológica de modo que solo los usuarios autorizados tengan acceso a los sistemas de UTMACH.
- Monitorear la red de forma que puedan detectar intentos de acceso no autorizado (registrando en documento el evento) y se pueda identificar cualquier actividad inusual en los servicios de acceso remoto por ejemplo:
    - Múltiples conexiones de una misma cuenta activadas a la vez.
    - Tráfico inusual (trafico fuera de las horas autorizadas para acceso remoto).
    - Considerar la configuración del sitio web.

Usuarios que requieran conectarse al acceso remoto:

- Solicitar acceso remoto al Director de tecnología.

- Asegurarse de que personas ajenas no utilicen dicha conexión para lograr acceso a los recursos informáticos de UTMACH.
- Utilizar herramientas tecnológicas con controles de seguridad para la conexión remota que puede ser Teamviewer versión 10 con licencia.

PROCEDIMIENTO.

1. El departamento de la Dirección de tecnología recibirá por correo electrónico la solicitud de servicios de acceso remoto.
2. Si la solicitud es para acceder a información de índole confidencial, se verificará que el usuario haya firmado un acuerdo de confidencialidad con UTMACH o que el acuerdo este incluido en el contrato firmado con UTMACH.
3. El Director de Tecnología determinará si la solicitud procede y cumple con los requerimientos, otorgando el acceso solicitado.
4. El administrador de la red o su delegado abrirá la cuenta del usuario, una vez reciba la solicitud autorizada por el Director de TI.
5. El administrador de la red notificará a la persona solicitante los códigos y claves de acceso correspondientes.
6. El administrador de la red desactivará la cuenta de usuario cuando el Director de TI solicite la desactivación, o cuando el administrador de red detecte alguna actividad sospechosa en la cuenta que pueda estar violando las normas de la Institución.
7. La empresa que está realizando soluciones a incidentes y / o problemas de los usuarios a través de una conexión segura a su equipo, tendrá la responsabilidad de documentar los cambios de acuerdo a procedimientos de cambios de software, el usuario que solicito el cambio debe validar el funcionamiento, y el administrador de la red debe verificar que los cambios fueron implantados de conformidad con lo documentado por el proveedor.
8. La empresa que está realizando soluciones a incidentes y /o problemas debe verificar que el usuario se encuentra presente frente a su equipo durante toda la sesión de asistencia remota (visualizando los cambios generados), el administrador de la red debe también estar visualizando los cambios realizados.

HITO 45 y 46 CONTROL DE ACCESO A USUARIOS TEMPORALES

Cada jefe departamental debe solicitar el usuario temporal a quien se debe autorizar y crear contraseña, el registro de solicitud debe tener la siguiente información.
Usuario, tiempo de vigencia de acceso, hora y fecha de inicio, hora y fecha de finalización, recursos a los que debe acceder.

La dirección de tecnología debe evaluar la solicitud, autorizar en caso de ser necesario, estar pendiente de revocar la autorización cuando se cumpla la hora y fecha de finalización.

HITO 47. PROCEDIMIENTO DE LOS MEDIOS DE RESPALDO, UNA VEZ CONCLUIDA SU VIDA ÚTIL RECOMENDADA POR EL PROVEEDOR Y LA DESTRUCCIÓN DE ESTOS MEDIOS

PROPÓSITO

Es habitual encontrar noticias en las que un usuario compra un disco duro o un portátil de segunda mano y acaba obteniendo información personal o incluso de alto secreto. Por estos riesgos es importante tener un procedimiento que permita garantizar que los dispositivos que ya no se vayan a utilizar por su vida útil sean correctamente destruidos para que nadie pueda acceder a información que en ellos se almacenaba.

ALCANCE

Incluye los discos duros de los equipos, cintas de copias, discos magnéticos como CD y DVD o memorias USB, inclusive también debemos tomar en cuenta la información que almacenamos en papel, que solemos desechar sin las adecuadas medidas de seguridad.

Por lo tanto antes de eliminar o reutilizar un soporte que haya almacenado información debemos aplicar las medidas de seguridad necesarias para evitar la recuperación de la información.

PROCEDIMIENTO

El personal de la Dirección tecnológica debe verificar si el dispositivo ha cumplido su vida útil o el usuario autorizado solicita por algún indicio la verificación del dispositivo.

Si vamos a reutilizarlo, donarlo, debemos realizar un borrado seguro del soporte. Es frecuente pensar que el borrado de la información o el formateo del disco duro elimina los datos, cuando esto no es cierto.

Al eliminar archivos utilizando la función suprimir habitual del sistema operativo, éste se limita a marcarlo como eliminado y la zona del disco que contenía sus datos como vacía. Es decir, los datos no han sido eliminados realmente. Siguen estando en el disco aunque a primera vista veamos el espacio como disponible. Y seguirán estando ahí hasta que nuevos datos ocupen esa zona de memoria.

Por este motivo, es posible recuperar cierta información que no ha sido borrada de manera segura. Existen herramientas capaces de leer el contenido del disco duro en una zona marcada como vacía, que pueden recuperar lo que había anteriormente en ella.

El Director de Tecnología tiene la responsabilidad de gestionar una herramienta tecnológica para borrar de forma segura los dispositivos, sugiero el uso de la herramienta KILLDISK que es un software que permite destruir todo el contenido del disco duro o disquete o memoria flash, sin posibilidad de volver a recuperar los ficheros o directorios borrados

El personal de la Dirección de tecnología tiene la responsabilidad de registrar el uso de la herramienta de borrado seguro, además de marcar el espacio como vacío, escriben en él datos aleatorios un número determinado de veces. De este modo, si una herramienta de recuperación intenta obtener el contenido anterior del disco duro lo que encontrará será los datos aleatorios y no la información original.

Si por el contrario vamos a desechar el soporte, debemos garantizar que nadie puede utilizarlo posteriormente, y que la información que contiene no puede ser recuperada.

El personal de la dirección de tecnología verificará si el dispositivo tiene mal funcionamiento, poca capacidad, antigüedad, porqué ya no es útil o porqué la información que contiene no es útil. Tampoco en este caso debemos pasar por alto los soportes en formato papel, que seguramente desechamos de manera regular.

Por ejemplo, es frecuente que las memorias USB dejen de funcionar por algún fallo en el conector, pero la información almacenada está intacta, y lo mismo es aplicable a los discos duros.

En general, la mejor opción para esto es hacer uso de la destrucción física del soporte. Para los soportes menos robustos (Cd, DVD, papel) podemos utilizar una destructora de papel.

HITO 48. PROCEDIMIENTO PARA QUE LA INFORMACIÓN SENSIBLE SEA PROTEGIDA DURANTE LA RECOLECCIÓN, PROCESAMIENTO Y ALMACENAMIENTO

DEFINICIONES.

- **Información sensible:** Para este documento se considera a la información confidencial (Reservada de uso interno, reservada confidencial y reservada secreta).

RESPONSABILIDADES.

Director de Tecnología:

- **Debe hacer cumplir las políticas de control de accesos:** Hitos correspondientes a CONTROL DE ACCESO con numeración 7 que reduce la posibilidad de filtraciones de información, se reducen las pérdidas accidentales por errores de usuarios, mejora el control sobre la información de la organización.
- **Debe hacer cumplir las políticas de copias de seguridad:** Evita la pérdida de información, facilita la respuesta frente a contingencias.
- **Debe hacer cumplir las políticas de seguridad de la información:** Cifrado de la información que protege los datos ante ataques informáticos y virus, evita que la información se pueda manipular, especialmente durante el tránsito de soportes,

reduce la difusión no autorizada de información, es un requisito legal para ciertos tipos de información.

- **Debe hacer cumplir los controles de eliminación de información:** Evita que se difunda información almacenada en soportes antiguos, imposibilita el acceso a los datos eliminados.
- **Debe verificar y hacer cumplir el Cláusulado legal:** mitiga el riesgo de que empleados o terceros hagan el uso inadecuado de la información, mejora el tratamiento de la información, es un requisito legal para los datos personales.

PROCEDIMIENTO.

Los usuarios de la UTMACH no deben dejar la información clasificada como Confidencial (Reservada de uso interno, reservada confidencial y reservada secreta) en lugares públicos.

Los usuarios de la UTMACH no deben dejar la información clasificada como Confidencial (Reservada de uso interno, reservada confidencial y reservada secreta) sin supervisión sobre su escritorio de las instalaciones de UTMACH.

La información clasificada como Confidencial (reservada interna)no debe difundirse a terceros salvo autorización expresa del Rector de la institución, esta información debe marcarse o etiquetarse adecuadamente

La información clasificada como Confidencial (reservada confidencial y reservada secreta), esta información debe estar marcada adecuadamente, se debe implementar todos los controles necesarios para limitar el acceso a la misma únicamente a aquellos empleados que necesiten conocerla. Esta información debe estar cifrada.

En caso de sacarla de las instalaciones de la empresa en forma digital, debe cifrarse.

No se admite el uso de archivos compartidos entre los equipos asignados, el envío y recepción de documentos internos se hará vía correo electrónico para que quede constancia del envió y de las partes relacionadas; de esta manera se asegura control sobre el flujo de comunicaciones internas de la UTMACH, manteniendo las políticas de correo electrónica (tamaño máximo permitido de los archivos).

El Director de Tecnología es responsable de implantar una solución tecnológica para archivar los documentos de acuerdo a su clasificación para que los usuarios puedan acceder mediante autenticación, en dicho repositorio considerar que la información

sensible esté cifrada, mediante este repositorio se podría mitigar el uso de espacio asignado para el correo electrónico.

Se debe habilitar ubicaciones físicas seguras para el almacenamiento de la documentación sensible. Los usuarios deben tener ubicaciones donde poder dejar la documentación al final del día. Estas ubicaciones pueden ser:

- Cajones de escritorio con llave.
- Despachos que se cierren con llave cuando no haya nadie
- Salas de archivo específicas
- Archivadores con llave.

Toda información considerada como confidencial en cualquiera de sus formas (impresos, electrónicos) deben estar provistas de la seguridad necesaria por quien la maneja para evitar el uso indebido por parte de personal no autorizado.

Para resguardar la información no se habilitarán dispositivos de grabación en medios magnéticos como grabadores de CD, DVD tampoco se habilitan los puertos USB para dispositivos masivo como Pendrive, discos externos, cámaras fotográficas, etc.

HITO 49. PROCEDIMIENTO DE REGISTRO DE INICIO SEGURO EVIDENCIAS.

- Registro de usuarios autorizados a aplicaciones autorizadas indicando cuales son privilegios especiales o críticas.
- Registros de cumplimiento de cambios de contraseña como lo estipula la política de control de acceso.

DEFINICIONES.

- **Servidores de dominio de autenticación:** En el servidor se registra los usuarios en el dominio, el usuario se autentica en el servidor de dominio a partir del cual se crea un canal seguro de comunicación con credenciales para verificar el usuario, asignándolo los privilegios correspondientes.

RESPONSABILIDADES.

AUTENTICAR USUARIOS AUTORIZADOS DE ACUERDO A LA POLÍTICA DE CONTROL DE ACCESO.

La dirección de tecnologías será responsable de controlar que todos los usuarios autorizados accedan a los recursos asignados por intermedio de un mecanismo de autenticación en cumplimiento de la política de acceso referenciado en los hitos mencionados en este documento.

Los usuarios autorizados tienen la responsabilidad de autenticarse a todas las aplicaciones autorizadas en cumplimiento con los documentos referenciales en este documento, documentos que establecen la política de control de acceso.

LLEVAR UN REGISTRO DE DEFINICION PARA EL USO DE PRIVILEGIOS ESPECIALES AL SISTEMA.

Los responsables de la Dirección Tecnológica deberán realizar el registro una vez por semana e informar al Oficial de la Seguridad de la Información. El registro debe realizarlo con el formulario de (REGISTROS DE AUDITORIA)

LLEVAR UN PROCESO DE MONITOREO Y REGISTRO DE LOS INTENTOS EXITOSOS Y FALLIDOS DE AUTENTICACIÓN DEL SISTEMA.

Los responsables de la Dirección Tecnológica deberán realizar el registro una vez por semana e informar al Oficial de la Seguridad de la Información. El registro debe realizarlo con el formulario REGISTROS DE AUDITORIA.

UTILIZAR MECANISMOS COMO USO DE DOMINIOS DE AUTENTICACIÓN.

El Director de tecnología es responsable de gestionar la implementación de servidores para dominios de autenticación. El área de tecnología configurará para que todos los usuarios autorizados de UTMACH accedan al sistema operativo a través del servidor de dominios de autenticación.

RESTRINGIR EL TIEMPO DE CONEXIÓN DE LOS USUARIOS CONSIDERANDO LAS NECESIDADES DE LA INSTITUCIÓN.

El jefe departamental deberá informar al Oficial de Seguridad de la Información la petición de restringir el acceso a ciertas horas y este solicitar a la Dirección de tecnologías que se proceda a aplicar la restricción.

Los jefes departamentales tendrán la responsabilidad de analizar si a un usuario autorizado deba restringirle el acceso a ciertas horas que pueda ser el horario de trabajo autorizado, pueda ser restringir el acceso a días laborables y no sábado y domingo. En caso necesario de que un usuario deba acceder fuera del horario establecido deba pedir autorización a su jefe departamental.

LIMITAR LA CANTIDAD DE INTENTOS PERMITIDOS DE REGISTRO DE INICIO DE SESIÓN.

La dirección de tecnologías deberá configurar en el servidor de dominios de autenticación para que el número de intentos permitidos de registro de inicio de sesión sean como máximo 3, si el usuario se pasa del número permitido el usuario quede bloqueado. Para activar el Jefe departamental deberá solicitar la habilitación al Oficial de Seguridad para que autorice y este solicite a la Dirección de tecnologías que se proceda a aplicar la habilitación.

El Director de Tecnologías deberá solicitar al desarrollador del sistema para que en las aplicaciones controle que el número de intentos permitidos de registro de inicio de sesión sean como máximo 3. Si el usuario se pasa del número permitido el usuario quede bloqueado. Para activar el Jefe departamental deberá solicitar la habilitación al Oficial de Seguridad para que autorice y este solicite al Área de tecnologías que se proceda a aplicar la habilitación.

Este mismo control deberá realizarse para el servicio de correo.

CONTROLAR QUE NO SE MUESTRE IDENTIFICADORES DE APLICACIÓN NI DEL SISTEMA.

El director de tecnología debe verificar que ninguna aplicación presente información sensible antes de que el usuario este autenticado, si lo presentare es responsabilidad de solicitar al proveedor que actualice la aplicación para llevar el control respecto de seguridad de la información.

Este proceso debe registrarse y controlarse como gestión de cambios para actualizar las versiones.

LIMITAR EL TIEMPO DE DILACIÓN ANTES DE PERMITIR O RECHAZAR MÁS INTENTOS ADICIONALES DE REGISTRO DE INICIO.

El área de tecnologías deberá configurar en los servidores de dominios de autenticación para que el período de tiempo tenga un tiempo limitado en el que se acumulan los intentos erróneos.

HITO 50. PROCEDIMIENTO PARA LA ADMINISTRACIÓN DE MEDIOS INFORMATICOS DE ALMACENAMIENTO

PROPÓSITO.

Definir las reglas para la protección de los datos en diferentes medios de almacenamiento y evitar la divulgación no autorizada, modificación, borrado o destrucción de los activos e interrupción de las actividades de negocio.

ALCANCE.

Se aplica a todos los usuarios de UTMACH, ya sean funcionarios, contratados, practicantes, consultores, incluyendo las empresas que presten servicios en UTMACH.

Aplica a todos los medios de almacenamiento removibles como son: Discos externos, pendrive, Cd y DVD, que hayan sido entregados por la UTMACH a los usuarios.

ROLES Y RESPONSABILIDADES.

- **Jefe Departamental:** Solicitar la asignación de medios removibles para personal de su dependencia.
- **Director de tecnología:** Evaluar y autorizar su uso.
- **Usuario:** debe mantener el debido resguardo de la información contenida en el medio removible que le fue asignado, informa de manera oportuna de cualquier deterioro, ocuparse de su uso, ubicación, análisis de virus, eliminación de datos en forma segura cuando corresponda.
- **Personal de la dirección de Tecnología:** Configurar a los PC no autorizados para denegar acceso a los medios removibles.

DESARROLLO.

1. Los usuarios no pueden utilizar un medio removible no autorizado y que no haya sido dado por la UTMACH.
2. Los usuarios solicitaran una ubicación con seguridad para el dispositivo
3. Los jefes departamentales solicitarán al jefe de área de tecnología la asignación de dispositivos indicando los motivos y qué tipo de información se usará en el almacenamiento.
4. Los usuarios tienen que escanear mediante antivirus cada vez que sea conectado a un equipo de UTMACH.
5. El director de tecnología en la entrega del dispositivo debe registrar el tiempo de vida útil para considerar su destrucción y eliminación correcta de la información.
6. La información almacenada en medios removibles que requiera estar disponible después del tiempo de vida del medio, debe ser almacenado en cualquier otro medio de manera de garantizar que no exista pérdida de información.
7. Toda vez que se requiera almacenar y transportar información sensible en medios removibles debe ser mediante herramientas de cifrado.
8. Cuando la información almacenada en un medio removible pierda vigencia, se debe formatear o destruir el medio en forma segura.
9. El personal de la dirección de Tecnología debe monitorear el buen uso de los dispositivos y en cumplimiento con la información antes detallada.
10. Los jefes departamentales en conjunto con director de tecnología deberán la pertinencia de restringir el acceso a los puestos USB, mediante configuración a nivel de software.

HITO 53,54,55. PROCEDIMIENTO PARA ADMINISTRAR LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

PROPOSITO

Los servicios de gestión de incidentes de seguridad de la información, están destinados a prevenir, detectar y solucionar incidentes de seguridad que atenten contra la confidencialidad, disponibilidad, integridad o autenticidad de la información, como es el caso de un incidente ocasionado por un código malicioso, un acceso no autorizado, una denegación de servicio o un uso inapropiado de los sistemas informáticos de la organización.

ALCANCE

Existen incidentes muy graves que pueden afectar la continuidad del negocio como son inundaciones, incendios, robos, etc.

La dirección de Tecnología de la Información debe socializar y comunicar un punto de contacto para la comunicación con el Responsable de la Dirección de Tecnologías.

Todos los empleados y terceros que presten algún servicio dentro de la UTMACH están obligados a reportar inmediatamente las deficiencias, vulnerabilidades, fallas o violaciones de seguridad que identifiquen durante el procesamiento, almacenamiento, intercambio o disposición de los activos de información, aún y cuando se trate de una simple sospecha.

Todos los reportes deberán ser manejados con estricta confidencialidad y podrán ser dados a conocer internamente siempre y cuando la Alta Dirección de la Dependencia así lo determine.

Queda estrictamente prohibido divulgar cualquier información sobre un incidente a personal externo a menos de que por disposiciones legales la dependencia se vea obligada a hacerlo. De ser así, deberá ser bajo la aprobación de la Alta Dirección de la Dependencia.

La persona que por negligencia no reporte a tiempo un incidente de seguridad o que aproveche deficiencias de seguridad y haga mal uso de la información, será sancionada de acuerdo a la gravedad.

Todos los usuarios tienen la responsabilidad de informar algún incidente ocurrido a los responsables de la Dirección de Tecnología de la Información mediante el llenado de una "Ficha de identificación y registro de incidentes" o bitácora de incidentes (incluyendo fecha, hora, con breve descripción del incidente, si lo envía por correo debe enviarlo al Responsable de la Dirección de Tecnología y este debe informar al Oficial de Seguridad de la información.

Los responsables de la Dirección de Tecnología tienen que registrar en un formulario denominado "Ficha de registro para tratamiento del incidente", donde se registra cada acción del incidente como: clasificarlo y darle el soporte inicial, si el incidente ya ha sucedido antes y se tiene en el historial de incidentes, con las acciones de solución se puede resolver y recuperar el incidente, si no existe en el historial, el personal de la Dirección de Tecnología debe realizar una investigación y diagnóstico quienes determinan si el incidente se categoriza como de alto riesgo, si no es de alto riesgo se procede a la solución ya sea con el personal de la Dirección de Tecnología o si es necesario escalar con una persona especializada en el tema.

El funcionario que está tratando el incidente debe escalar en caso de ser necesario el incidente al Director de Tecnología quien debe gestionar la participación de personal externo.

Una vez realizada la solución, si ésta generó cambios, es importante que se aplique la gestión de cambios evidenciando todos los cambios como se muestra en los hitos 1 al 35.

El funcionario a cargo del incidente debe registrar en el historial de incidentes, hasta llegar al cierre del mismo, el cual debe comunicarse al usuario que el incidente ha sido resuelto.

El funcionario a cargo de la solución del incidente debe actualizar el estado del incidente en el registro de tratamiento del incidente.

En el caso de que el incidente sea considerado como de alto riesgo, es importante tener los contactos con las autoridades como la policía, fiscalía, etc., tener acuerdos de

cooperación, como se detalla en el listado de "Clasificación de los tipos de incidentes", se debe considerar llamar a la autoridad competente.

DEFINICIONES:

Clasificación del Incidente: Al incidente se lo clasificará por el tipo de servicio afectado y por el nivel de severidad, para la resolución del incidente.

El nivel de severidad se basa esencialmente en dos parámetros:

- **Impacto del incidente:** determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados.
- **Impacto en el tiempo:** depende del tiempo máximo de demora que acepte el usuario para la resolución del incidente.

También se deben tener en cuenta factores auxiliares tales como el tiempo de resolución esperado y los recursos necesarios: los incidentes "sencillos" se tramitarán cuanto antes.

Dependiendo de la prioridad se asignarán los recursos necesarios para la resolución del incidente.

La prioridad del incidente puede cambiar durante su ciclo de vida. Por ejemplo, se pueden encontrar soluciones temporales que restauren aceptablemente los niveles de servicio y que permitan retrasar el cierre del incidente sin graves repercusiones.

Es conveniente establecer un protocolo para determinar, en primera instancia, la prioridad del incidente. El siguiente diagrama nos muestra un posible "diagrama de prioridades" en función de la urgencia e impacto del incidente:

Escalar el incidente: Si la Dirección de Tecnología no está en condiciones de resolver en primera instancia un incidente y para ello deba recurrir a un especialista o a algún superior que pueda tomar decisiones que se escapan de su responsabilidad. A este proceso se le denomina escalado.

Tipos de Incidentes:

- ✓ Fraude y robo de activos de información o de cómputo.
- ✓ Divulgación, manipulación, destrucción o modificación no autorizada de la información de la compañía.
- ✓ Interrupción de procesos y sistemas críticos del negocio.
- ✓ Fallas en la seguridad de los sistemas de información.

- ✓ Fallas en la seguridad física de las instalaciones.
- ✓ Deficiencias o mal funcionamiento de los sistemas.
- ✓ Acceso no autorizado a los recursos de la compañía.
- ✓ Uso indebido de los privilegios dentro de un sistema.
- ✓ Propagación de virus o código malicioso.
- ✓ Intrusiones externas a la red (hackeo).
- ✓ Instalación de software no autorizado por la UTMACH.
- ✓ Uso irracional de los recursos informáticos de la UTMACH.

FICHA PARA REGISTRAR EL TRATAMIENTO DE INCIDENTES

ID Incidente:		
Fecha y hora		
Nombre del Funcionario		
Departamento		

Estado

Registrado	
En ejecución	
Suspendido	
Resuelto	
Cerrado	

Clasificación por:

Nivel de prioridad

Impacto:	Alto	medio	Bajo
Urgencia:			

Diagnostico

Resolución

Causas por la que ocurrió el incidente	

Escalar Incidente	Si	No

Si la respuesta es si

Genero gestión cambios

Si

No

Jefe de Área de Tecnología Información

Personal de Tecnología

Oficial de Seguridad de la

HITO 56-60. MANUAL PARA REALIZAR EVALUACIÓN DE RIESGOS

Todo el proceso de evaluación de riesgos debe ser apoyado por la alta dirección, elaborado por la gerencia de sistemas y el administrador de la red; así mismo se le debe dar a conocer y debe ser monitoreado por el oficial de seguridad de la información.

La evaluación de riesgos se realizará siguiendo la metodología propuesta por la norma ISO 27001:

PASO 1: Determinación del alcance

La determinación del alcance la realizarán: el responsable de la gerencia de sistemas y el administrador de la red de UTMACH.

- Se debe determinar si la evaluación de riesgos se aplica a los sistemas, red, dominios de la norma iso 27001, etc.

PASO 2: Identificación de activos

Se entiende por activo algo a lo que la organización directamente le asigna un valor y por tanto la organización debe proteger.

Para el alcance definido se deben identificar los activos asociados, básicamente se deben considerar tres tipos de activos: Información, Hardware, Software, Personal.

Información.- Datos relevantes que puedan estar contenidos en cualquier soporte electrónico, magnético u óptico, incluso en la memoria del personal responsable.

Hardware.- Dispositivos etc. que forma parte del alcance definido.

Software.- Aplicaciones, Sistemas operativos, etc.

Personal.- Responsable del funcionamiento, mantenimiento u operación en general del alcance definido.

Por ejemplo, si se define el segmento de red WLAN (red de área local inalámbrica):

Id. De segmento	**Segmento de red crítico**	**ACTIVOS**			
		Información	**Hardware**	**Software**	**Personal**
	RED DE ÁREA LOCAL	Documentación de la	Puntos de acceso	Aplicación para la	Administrad

	INALÁMBRICA	distribución física de los puntos de acceso inalámbricos	inalámbricos (AP), AP1, AP2	administración de los AP.	or de red

PASO 3: Tasación de activos

Será necesario que a cada uno de los activos asociados al alcance se le dé un valor (tasar el activo), basándose en los pilares de la seguridad de la información, Confidencialidad, Integridad y Disponibilidad; para esto se puede utilizar una escala de Likert. El valor 1 significa "muy poco" y 5 "muy alto". Para utilizar la escala se puede realizar la siguiente pregunta: **¿Cómo una pérdida o una falla en un determinado activo afecta la confidencialidad, la integridad y la disponibilidad?**, luego se tendrá un Total que es el promedio de las calificaciones obtenidas.

La calificación debe ser asignada por el responsable de sistemas, el administrador de la red y los operadores de la misma quienes tienen conocimiento de los detalles del alcance definido

Por ejemplo:

Segmento de red crítico	**Activos**	**Tasación**			
		Confidencialidad	**Integridad**	**Disponibilidad**	**Total**
RED DE ÁREA LOCAL INALÁMBRICA	Documentación de la distribución física de los puntos de acceso inalámbricos	4	1	1	2
	AP1	4	4	5	4.3
	AP2	4	4	5	4.3
	…				

PASO 4: Identificación de amenazas

Una amenaza es un evento adverso que puede afectar la consecución de los objetivos de una organización.

Podemos clasificar a las amenazas en:

Naturales (inundaciones, sismos, etc.)

Intencionales (huelgas, vandalismo, hacking, etc.)

Involuntarias (daño por desconocimiento o falta de capacitación)

Siguiendo la metodología se debe determinar las amenazas a las que están expuestos los activos.

Será el responsable de sistemas, el administrador de red y los operadores de la misma quienes identifiquen las amenazas y luego midan la posibilidad de su ocurrencia, pueden utilizar la escala de Likert mencionada en el documento. Para la medición pueden acudir a la revisión de históricos de eventos, comparación con información de otras entidades que tienen la misma dedicación o cuya infraestructura sea similar, etc.

Ejemplo de identificación de amenazas y calificación de la posibilidad de ocurrencia de las mismas:

Segmento de red crítico	Activos	Amenazas	Posibilidad de ocurrencia de amenaza
RED DE ÁREA LOCAL INALÁMBRICA	Documentación de la distribución física de los puntos de acceso inalámbricos	Deterioro, ilegibilidad	**2**
		Robo	**1**
		Traspapeleo	**2**
	AP 1	Daño del equipo	**3**
		Hurto de equipo	**1**
	…		

PASO 5: Identificación de vulnerabilidades

Una vulnerabilidad es una debilidad de los activos que puede hacer que una amenaza se materialice.

Será el responsable de sistemas, el administrador de red y los operadores de la misma quienes identifiquen las vulnerabilidades de los activos, para esto puede ayudar de mucho la pregunta ¿Cuál amenaza pudiese explotar cuál de las vulnerabilidades?

Luego es necesario evaluar la posibilidad de que las vulnerabilidades sean explotadas por las amenazas, se puede utilizar la escala de Likert mencionada en el documento.

Ejemplo de identificación de vulnerabilidades y calificación de la posibilidad de que amenaza explote la vulnerabilidad:

Segmento de red crítico	Activos	Amenazas	Posibilidad de ocurrencia de amenaza	Vulnerabilidad	Posibilidad de que amenaza explote la vulnerabilidad
RED DE ÁREA LOCAL INALÁMBRICA	Documentación de la distribución física de los puntos de acceso inalámbricos	Deterioro, ilegibilidad	2	Ambiente de custodia insalubre	**3**
		Robo	1	Inexistencia de seguridad física	**5**
		Traspapeleo	2	Ambiente de custodia desordenado	**5**
	AP 1	Daño del equipo	3	Equipos sin garantía	**4**
				Equipo sin contrato de soporte técnico	**4**
		Hurto de equipo	1	Inexistencia de seguridad física	**5**
	…				

PASO 6: Determinación y priorización del riesgo

Para determinar y priorizar el riesgo (Alto, Medio o Bajo):

1) Obtener el valor de “Posible ocurrencia de amenaza y vulnerabilidad” que es el resultado del promedio entre “posibilidad de ocurrencia de amenaza” y la “posibilidad de que amenaza explote la vulnerabilidad”

Segmento de red crítico	Activos	Posibilidad de ocurrencia de amenaza	Posibilidad de que amenaza explote la vulnerabilidad	Posible ocurrencia de amenaza y vulnerabilidad
RED DE ÁREA LOCAL	Documentación	2	3	**2.5**

INALÁMBRICA	de la distribución física de los puntos de acceso inalámbricos	1	5	**3**
		2	5	**3.5**
	AP 1	3	4	**3.5**
			4	
		1	5	**3**
	…			

2) Por último el valor del riesgo será resultado del promedio entre el "valor del activo" que es el resultado de la tasación del Paso 3 y la "posible ocurrencia de amenaza y vulnerabilidad"

Segmento de red crítico	Activos	Valor del activo	Posible ocurrencia de amenaza y vulnerabilidad	TOTAL
RED DE ÁREA LOCAL INALÁMBRICA	Documentación de la distribución física de los puntos de acceso inalámbricos	2	2.5	**2,5**
			3	
			3.5	
	AP 1	4.3	3.5	**3,8**
			3	
	…			

3) Se puede priorizar el riesgo usando la escala de Likert:

De 1.0 a 2.3 Riesgo de criticidad baja.
De 2.4 a 3.6 Riesgo de criticidad media
De 3.7 a 5.0 Riesgo de criticidad alta

Segmento de red crítico	Activos	Valor del activo	Posible ocurrencia de amenaza y vulnerabilidad	TOTAL	Criticidad
RED DE ÁREA LOCAL INALÁMBRICA	Documentación de la distribución física de los puntos de acceso inalámbricos	2	2.5 3 3.5	2,5	**Media**
	AP 1	4.3	3.5 3	3,8	**Alta**
	…				

Hasta este punto se habrán evaluado y priorizado los riesgos por criticidad.

PASO 7: Tratamiento del riesgo

Debieran tratarse inicialmente los riesgos de criticidad “Alta”, los de criticidad “Media” y “Baja” se recomienda tomarlos en cuenta en evaluaciones posteriores las cuales se pueden realizar en un plazo no mayor a un año; en el mejor de los casos todos los riegos deberían ser tratados.

Las opciones de tratamiento del riesgo son:

Mitigar el riego.- Que es la implementación de controles que reduzcan la probabilidad de amenaza.

Asumir el riesgo.- Que es aceptar el riesgo y continuar operando como se ha estado haciendo.

Eliminar el riesgo.- Que es eliminar la causa del riesgo, por ejemplo sacar de producción el activo.

Transferir el riesgo.- Que es el uso de opciones que compensen la pérdida, por ejemplo adquirir pólizas de seguros.

El departamento de sistemas junto al administrador de la red son los responsables de elaborar la propuesta de tratamiento, propuesta que será socializada al oficial de seguridad de la información y si el caso amerita (como por ejemplo el alto costo que pueda suponer) exponerla a la alta gerencia para tomar la mejor decisión.

Segmento de red crítico	Activos	Criticidad	Opción de tratamiento	Criticidad	Observaciones
RED DE ÁREA LOCAL INALÁMBRICA	Documentación de la distribución física de los puntos de acceso inalámbricos	Media	Aceptar	**Media**	Inicialmente se tratarán los riegos de criticidad alta
	AP 1	Alta	Mitigar	**Alta**	
	…				

PASO 8: Enunciado de aplicabilidad

Para cuando se ha decidido "mitigar" el riesgo se debe elaborar un enunciado de aplicabilidad que es el documento en el que se deja constancia de los controles a implementar la fecha de implementación, el responsable de la implementación y alguna observación si lo amerita esto por cada activo de criticidad alta.

Segmento de red	Activo	Control	Fecha de implementación	Responsable	Observación
Red de área local inalámbrica	Punto de acceso (AP1)	Mantenimiento preventivo del equipo	--/--/----	Operador de la red	Se debe contar con un cronograma para el mantenimiento de los dispositivos inalámbricos.

El enunciado es elaborado por la gerencia de sistemas y el administrador de la red, además debe ser aprobado por la dirección y conocido por el oficial de seguridad de la información para las actividades de seguimiento y así garantizar la implementación.

Para la selección de controles se debe considerar la efectividad de los mismos, el costo-beneficio, que sean confiables que no estén en contra de la legislación y las regulaciones y que de ninguna forma detengan el normal desarrollo de las operaciones.

El cumplimiento del enunciado de aplicabilidad debiera ser monitoreado por el oficial de seguridad de la información y se debe tomar en cuenta para futuras evaluaciones del riesgo.

GLOSARIO:

Activo.- Es algo que tiene valor o utilidad para la organización o departamento de la organización, sus operaciones comerciales o su continuidad.

Amenaza.- Es un potencial evento no deseado.

Confidencialidad.- propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Crítico.- Es indispensable para la operación de la empresa.

Disponibilidad.- propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

DMZ (Zona desmilitarizada).- es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa.

Enunciado de aplicabilidad.- documento que describe los controles pertinentes y aplicables para mitigar los riesgos.

Granja de servidores.- es un grupo de servidores, normalmente mantenidos por una empresa para ejecutar tareas que van más allá de la capacidad de una sola máquina.

Integridad.- propiedad de salvaguardar la exactitud y estado completo de los activos.

Segmento de red.- Puede ser definido físicamente como un conjunto de dispositivos que tengan como límite la interfaz de un router o un servidor de aplicaciones; o lógicamente como una subred IP que es un tipo de red de área local virtual.

Tasar activo.- Darle valor al activo, para la seguridad de la información la tasación se debe basar en la confidencialidad, integridad y disponibilidad.

VLAN (Red de área local virtual).- es una forma para crear redes lógicas independientes dentro de una misma red física, por ejemplo una subred IP.

Vulnerabilidad.- Es una vulnerabilidad en la infraestructura que puede ser explotada por las amenazas.

CAPÍTULO VI

6.1 CONCLUSIONES

- Los objetivos planteados en este estudio se cumplieron en su totalidad, evidenciados mediante los resultados alcanzados en los niveles de capacidad de los procesos que propone COBIT5.0, además de establecer los procesos prioritarios mediante la aplicación de Cascada de metas que permite introducir las preocupaciones de la institución a través del comité evaluador de procesos y finalmente realizar el plan de acción que establece las actividades a desarrollar para mejorar el nivel de capacidad evidenciados con productos entregables, de tal manera que la institución pueda decidir la implementación de acuerdo a sus necesidades.
- El estudio realizado permite a la Institución identificar el nivel de capacidad de los procesos respecto a las Tecnologías de la Información, además de establecer los procesos prioritarios que permita generar proyecciones de implementación de los mismos para mejorar la gestión estratégica que permita crear valor y minimizar los riesgos.
- Destacar la colaboración por parte de la Institución ya que a través del comité evaluador de procesos existió la participación en forma directa en la toma de decisiones para definir (i) la existencia de actividades en la auditoria de cumplimiento de los procesos, (ii) las necesidades de las partes interesadas, (iii) seleccionar las actividades para mejorar el nivel de capacidad.
- El trabajo también puede servir a cualquier organización que quiera emprender en el proceso de implementación de los procesos de COBIT5.0, ya que está elaborado como guía donde se detalla los pasos que se debe seguir.
- El promedio de 29,75% obtenido como resultado del nivel de capacidad de los procesos refleja el estado actual de la institución en cuanto a la gestión de los procesos de TI, donde es necesario al apoyo de las altas autoridades para crear la estructura organizacional de TI capaz de promover la implementación en forma progresiva y estratégica de los procesos.

- Para obtener el nivel de capacidad de los procesos se aplicó una entrevista con un gran volumen de preguntas por cada proceso (29 procesos) y por asunto tiempo genero dificultades para la aplicación de las mismas; lo cual puede producir un sesgo en los resultados obtenidos.
- El valor de 29,75% refleja el nivel de capacidad promedio de los procesos cuyo resultado refleja un porcentaje alcanzado parcial, con muchas debilidades en forma general, que es necesario plantearse muchos objetivos para mejorar y poder llegar al menos a superar el nivel 1 de las capacidades.
- Al existir muchos procesos con el nivel de capacidad muy bajo, reflejando muchas necesidades de cambio en los procesos de TI y de acuerdo a la metodología de este trabajo de escoger tres preguntas por parte de los interesados para determinar los procesos prioritarios pudo provocar un sesgo en este caso por aspectos de seguridad.

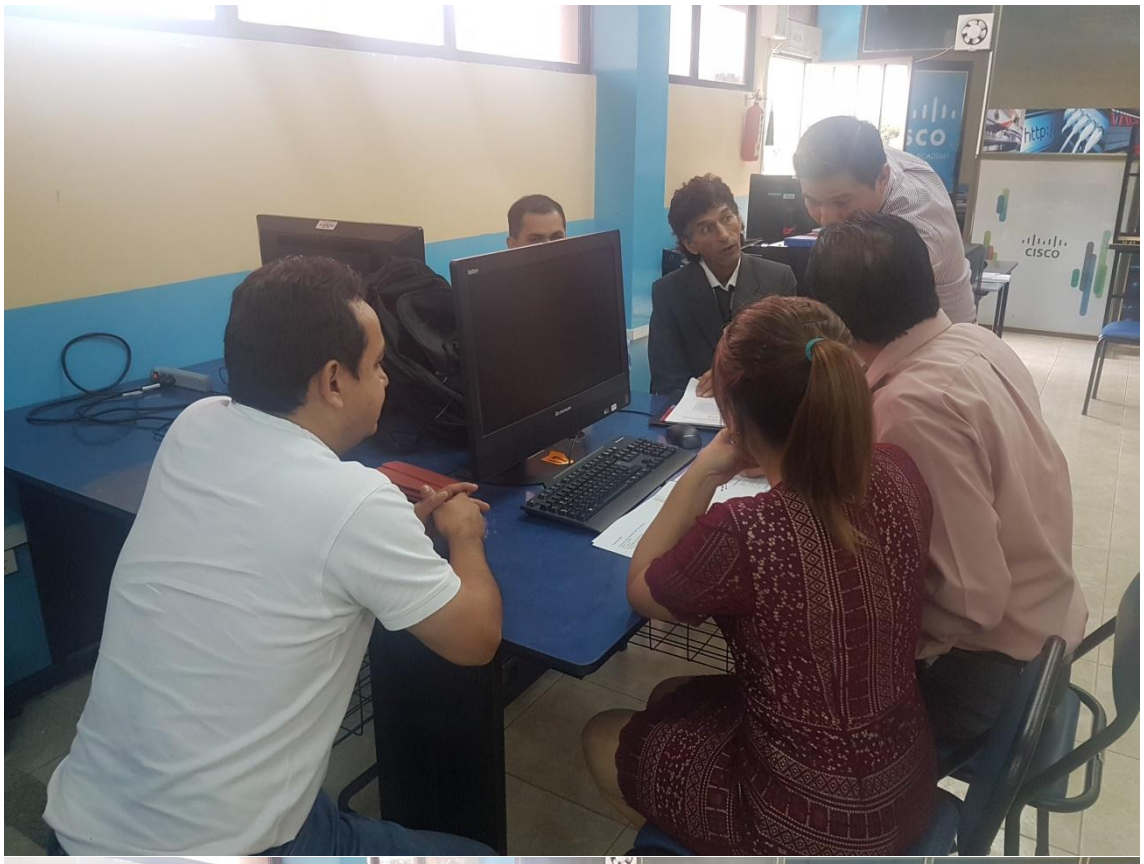
6.2 RECOMENDACIONES

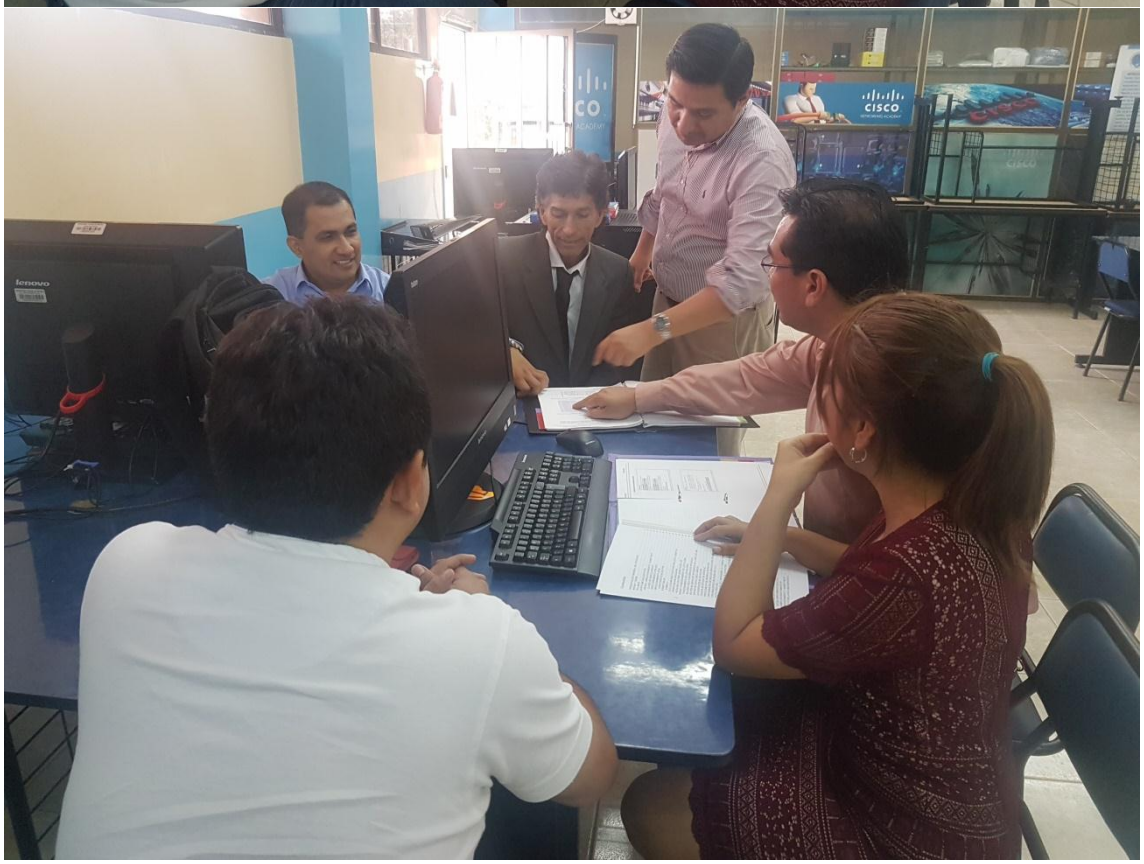
- Es importante establecer una adecuada socialización del proyecto de implementación de COBIT5.0 en la institución para generar el apoyo de las partes interesadas.
- La institución debe acoger el estudio realizado como una puerta abierta que permita mejorar la gestión de TI mediante la creación de valor y minimizar los riesgos.
- La información obtenida debe ser validada, ya que por tema tiempo se pudo generar sesgo, a pesar de la colaboración de la Institución muy proactiva del comité evaluador de procesos conformada por personal de las partes interesadas de la institución.
- A futuro, plasmar este trabajo en un libro para que pueda servir a cualquier organización que quiera emprender en el proceso de implementación de los procesos de COBIT5.0.
- De acuerdo al promedio de 29,75% obtenido como resultado del nivel de capacidad de los procesos se recomienda el apoyo de las altas autoridades para crear la estructura organizacional de TI capaz de promover la implementación en forma progresiva y estratégica de los procesos.
- De acuerdo al promedio de 29,75% obtenido como resultado del nivel de capacidad de los procesos se recomienda el apoyo de las altas autoridades para crear políticas institucionales que permitan establecer un entorno de recursos para que se viabilice el proyecto de implementación de Cobit5.0.
- Finalmente, se recomienda a la institución de que este trabajo no quede en archivo, sino se implemente a corto plazo, y se plantee progresivamente en el tiempo crear un plan de acción para mejorar todos los procesos de CObit5.0 de tal manera que la Tecnología de la Información sea vista como lo que debe ser, esto es estratégica que permita estar alineado a los objetivos institucionales, y no ser simplemente soporte.

ANEXOS

ANEXO A.

REUNIONES DE TRABAJO CON COMITÉ EVALUADOR DE PROCESOS.


CISCO


CISCO
lenovo

BIBLIOGRAFÍA

(UE), O. I. (2004). *Evaluación de los enfoques para integrar la sostenibilidad a las políticas comunitarias.*

America, I. l. (2014). gobierno de TI. *SISTEMAS*.

Baquerizo Anastacio, M. M. (2014). *Modelo de seguridad para sistemas E-Gobierno Mediante Satisfacilidad Booleana.* (J. A. Martín Hernández, Ed.) Recuperado el 5 de Julio de 2016, de Trabajo Fin de Máster en Ingenieria Informática para la Industria Universidad Complutense de Madrid: http://eprints.ucm.es/24485/1/MONICA%20MARLENE%20BAQUERIZO%20ANASTACIO.pdf

Bengtsson, F., & Ågerfalk, P. J. (Septiembre de 2010). Information technology as a change actant in sustainability innovation: Insights from Uppsala. *Elsevier*.

Bjoern, M., Koray, E., Fabian, L., & Ruediger, Z. (Agosto de 2013). How Sustainable is COBIT 5? *Americas Conference on Information Systems:, 19*, 15-17.

Brundtland, G. H. (1987). *Comisión de las Naciones Unidas sobre el Medio Ambiente Mundial y el Desarrolllo.*

Chaudhuri, A. (2011). ENABLING EFFECTIVE IT GOVERNANCE: LEVERAGING ISO/IEC 38500:2008 AND COBIT TO ACHIEVE COBIT TO ACHIEVE BUSINESS–IT ALIGNMENT. *The EDP Audit, Control, and Security Newsletter, 44*(2), 1-18.

DUX DILIGENS. (2012). *Gestión de Servicios de TI.* Recuperado el 14 de Junio 28 de 2016, de http://52.0.140.184/typo43/fileadmin/Conferencias/GestiondeTIconSoftwareLibreOTRS.pdf

ECONOMICO, O. P. (2011). *Directrices de la OCDE SOBRE EL GOBIERNO CORPORATIVO DE LAS EMPRESAS PUBLICAS.*

Eka Putri, R., & Surendro, K. (16-19 de Noviembre de 2015). Un modelo de evaluación de la capacidad del proceso de gobierno de TI basado en la norma ISO 38500. Recuperado el 5 de Julio de 2016, de http://ieeexplore.ieee.org.accedys.udc.es/xpls/icp.jsp?arnumber=7437673

Fernández, A., & Llorens, F. (2011). *Gobierno de las TI para universidades.* Recuperado el 5 de Julio de 2016, de TIC Comision Sectorial de las Tecnologías de la información y las Comunicaciones: http://tic.crue.org/wp-content/uploads/2016/04/gobierno_de_las_TI_para_universidades.pdf

Folgueras Marcos, A., & Santiago Ramirez, D. (2010). *Análisis y Estudio sobre el gobierno y gestión de los servicios de TI en el Mercado español 2008-2010.* Madrid: Repositorio Universidad Carlos III de Madrid.

G. Braga, C. C. (26 de Octubre de 2015). *Abordando la sostenibilidad y responsabilidad social en los proceso de gobierno de TI de COBIT 5*. (ISACA) Recuperado el 03 de Julio de

2016, de http://www.isaca.org/COBIT/focus/Pages/addressing-sustainability-and-social-responsibility-in-cobit-5-it-governance-processes-spanish.aspx

Gantman, S., & Fedorowicz, J. (Mayo de 2016). Communication and control in outsourced IS development projects: Mapping to COBIT domains. *Elsevier, 21*, 63-83.

GERENCIA, R. (2013). GOBIERNO DE TI PARA OBTENER EL MAYOR VALOR DE LAS TI. *GERENCIA*.

Graciela Braga, C. C. (2015). THE TIME FOR SUSTAINABLE BUSINESS IS NOW: LEVERAGING COBIT 5 IN SUSTAINABLE BUSINESS. *ISACA JOURNAL, 3*.

Haris Hamidovic, C. (2011). *Fundamentos del Gobierno de TI basados en ISO/IEC 38500 ISACA.*

Internacional, F. M. (19 de Enero de 2016). Los principales riesgos para la economía mundial en 2016 y 2017, según el FMI. *RT News*.

Iraldo, F., Testa, F., & Frey, M. (2009). Es un sistema de gestión medioambiental capaz de influir en el comportamiento medioambiental y competitivo? El caso del sistema comunitario de gestión y auditoría medioambientales (EMAS) en la Unión Europea. *Journal of Cleaner Production, 17*(16), 1444-1452. doi:10.1016 / j.jclepro.2009.05.013

ISACA. (2012). *COBIT 5 "Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa".*

ISACA. (2012). *ISACA.* Obtenido de https://issuu.com/martingarcia25/docs/cobit5-enabling-spanish

ISACA. (2012). Modelo de Cascada de metas .

ISACA. (2012). *procesos catalizadores.*

ISACA. (2013). *Cobit 5.0 Self Assessment Templates en español.* Obtenido de https://es.scribd.com/docuemnt/168025529/3-cobit-5-self-assessment-templates

ISACA. (2016). *PAM-Using cobit 5 Toolkit-tkt_eng_0114.*

ISACA, R. M. (2011). *Artículo Técnico de Sostenibilidad.*

ISO/IEC. (2015). *ISO/IEC 38500: Tecnologia de la información - Gobierno de TI para la organización.* Suiza: ISO/IEC.

ITGI. (2008). 50% DE LOS PROYECTOS IT SON ELIMINADOS ANTES DE IMPLEMENTARSE. *latin America CACS.* Chile.

J.Calvo-Manzano, G.Cuevas, M.Muñoz, & T.San Feliú. (2008). Estudio entre modelos y estándares de buenas prácticas enfocado a las prácticas de planificación de proyectos y utilizando CMMI como referencia. *Conferencia Ibérica de Sistemas y Tecnologías de la Información CISTI.* Ourense,España.

Laksono, H., & Supriyadi, Y. (Noviembre de 2015). Design and Implementation Information Security Governance Using Analytic Network Process and COBIT 5 For Information Security. *IEEE*, 17.

Lerch Lunardi, W., Luiz Becker, J., & Gastaud Maçada, A. (14 de Febrero de 2012). Un estudio empírico sobre el impacto de la gobernabilidad de TI en el desempeño organizacional. *Produção, 22*(3), 14. doi:http://dx.doi.org/10.1590/S0103-65132012005000003

Llorens, A. F. (2011). Gobierno de las TI en las Universidades Españolas. *Repositorio Institucional de la Universidad de Alicante*.

Machado, M. C., Sobral, F. A., & Junior, F. H. (2014). Sustentabilidade na tecnologia da informacao análise dos aspectos considerados no modelo de cobit. *IV SINGEP*.

Meaddows, R. (2008). Principales problemas de gobierno de TI.

Megias, J. (29 de Junio de 2009). Gobierno de las TI. *Estrategias, Strtups y modelos de negocio*.

Merhout, J. W., & O'Toole, J. (Julio de 2015). Sustainable IT Governance (SITG): Is COBIT 5 An Adequate Model? *AIS Electronic Library*, 1-7.

Mohamad, S., & Toomey, M. (2016). A survey of information technology governance capability in five jurisdictions using the ISO 38500:2008 framework. *International Journal of Disclosure and Governance, 13*(1), 53-74.

Monica Isabel Bayas Condo, W. G. (2014). Desarrollo de un modelo de madurez tecnologico. *Fuerzas Armadas, Ecuador*.

Neto, J. S., & Neto, A. N. (Diciembre de 2013). Metamodel of the IT Governance Framework COBIT . *JISTEM: Journal of Information Systems and Technology Management, 10*(3), 521-540.

NETWORK, I. G. (2011). Understanding the cobit 5 process Assessment Model. *IT GOVERNANCE NETWORK*.

Oliver, D., & Lainhart, J. (Agosto de 2012). COBIT 5: Adding Value Through Effective Geit. *EDPACS, 46*(3), 1-12.

P. Weill, J. R. (2004). *IT Governance How Top Performers Manage IT Decision Rights for Superior Results.* Massachusetts: Harvard Business School Press.

Pedrosa Ortega, C. (2009). Modelos teóricos que nos ayudan a comprender el gobierno de las sociedades cooperativas, una apuesta por el enfoque de los stakeholders. *Gestión Jovén: Revista de la Agrupación Jovén Iberoamericana de Contabilidad y Administracion de Empresas (AJOICA)*(4), 2-5.

Putri, R., & Surendro, K. (2015). A Process Capability Assessment Model of IT Governance Based on ISO 38500. *IEEE*, 1-6.

Standing, C., & Jackson, P. (2007). An approach to sustainability for information systems. *Journal of Systems and Information Technology, 9*, 167-176.

Stefan Naumann, M. D. (2011). The GREENSOFT Model: A reerence model for green and sustainable software. *Elsevier*.

Symons, C., Cecere, W. M., Young, O. G., & Lambert, N. (29 de Marzo de 2005). *Symons C - Forrester Research, 2005 - i.bnet.com.* Recuperado el 23 de Julio de 2016, de www

Tsai, W.-H., Hsieh, C.-L., Wang, C.-W., Chen, C.-T., & Li, W.-H. (2015). The Impact of IT Management Process of COBIT 5 on Internal Control. *IEEE*.

Universidad Técnica de Machala. (2017). *utmachala*. Obtenido de http://www.utmachala.edu.ec/portalwp/

Velásquez Pérez, T., Puentes Velásquez, A. M., & Pérez Pérez, Y. M. (Diciembre de 2015). Un enfoque de buenas prácticas de gobierno corporativo de TI. *Tecnura, 19*, 159-169. Recuperado el 05 de Julio de 2016, de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2015000500015&lang=pt

Weill, P., & Woodham, R. (Abril de 2002). Don't Just Lead, Govern: Implementing Effective IT Governance. *Social Science Research Network, 3*(326).