UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado:

"PROPUESTA DE NORMATIVA BASADA EN COBIT, PARA EL CONTROL INTERNO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL SECTOR PÚBLICO ECUATORIANO"

Realizado por:

FERNANDO JAVIER FIGUEROA SIMBAÑA

LUCIA GABRIELA HINOJOSA JARAMILLO

Directora de proyecto:

MSC. VERÓNICA RODRÍGUEZ

Como requisito para la obtención del título de:

MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDADES DE REDES Y COMUNICACIÓN

Quito, abril del 2018

DECLARACIÓN JURAMENTADA

Nosotros, FERNANDO JAVIER FIGUEROA SIMBAÑA, con cédula de ciudadanía 1715119853, y LUCIA GABRIELA HINOJOSA JARAMILLO, con cédula de ciudadanía 1715140206, declaramos bajo juramento que el trabajo aquí desarrollado es de nuestra propia autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, se cede los derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente

Fernando Javier Figueroa Simbaña

C.C.: 1715119853

Lucía Gabriela Hinojosa Jaramillo

C.C.: 1715140206

DECLARATORIA

El presente trabajo de investigación titulado:

"PROPUESTA DE NORMATIVA BASADA EN COBIT, PARA EL CONTROL INTERNO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL SECTOR PÚBLICO ECUATORIANO"

Realizado por:

FERNANDO JAVIER FIGUEROA SIMBAÑA

LUCIA GABRIELA HINOJOSA JARAMILLO

ha sido dirigido por la docente:

MSC. VERÓNICA RODRÍGUEZ

quien considera que constituye un trabajo original de su autor

Msc. Verónica Rodríguez Arboleda

DIRECTORA

LOS PROFESORES INFORMANTES

Los Profesores Informantes:

Msc. EDISON ESTRELLA

Msc. FABIAN HURTADO VARGAS

Después de revisar el trabajo presentado,

lo han calificado como apto para su defensa oral ante el tribunal examinador

Edison Estrella Fabián Hurtado Vargas

Quito, abril del 2018

DEDICATORIA

Dedico el presente trabajo de investigación a mi esposa fuente de inspiración y apoyo constante en mi formación profesional; a mis padres quienes cultivaron valores y principios que han guiado mi crecimiento personal, y a mi abuelito quien desde el cielo siempre me acompaña.

Fernando Figueroa.

Dedico el presente trabajo de investigación a mis padres que han sido el apoyo en cada momento de mi vida y me han enseñado a no decaer ante las adversidades, a mi esposo por ser siempre el soporte incondicional en cada proyecto que decido emprender, a mis hijas por ser la motivación para ser una mejor persona y profesional, y a mi hermana por ser mi compañera fiel en los tiempos difíciles.

Gabriela Hinojosa.

AGRADECIMIENTO

A la profesora Verónica Rodríguez por su acertada dirección de la tesis. Su profesionalismo, dedicación y entrega fueron determinantes a la hora de conformar este documento.

A los profesores Edison Estrella y Fabián Hurtado, como lectores quienes con su amplia experiencia y conocimientos aportaron una visión integradora a nuestro trabajo de investigación.

A la Universidad Internacional SEK, por su esfuerzo de innovar y formar profesionales íntegros.

ÍNDICE GENERAL DE CONTENIDO

DECLARACIÓN JURAMENTADA ... ii
DECLARATORIA ... iii
LOS PROFESORES INFORMANTES ... iv
DEDICATORIA ... v
AGRADECIMIENTO ... vi
Resumen ... xii
Abstract ... xiii
CAPÍTULO I ... 1
1.1 PROBLEMA DE LA INVESTIGACIÓN ... 1
1.1.1 Planteamiento del Problema ... 1
1.1.1.1 Diagnóstico ... 1
1.1.1.2 Pronóstico ... 3
1.1.1.3 Control de Pronóstico ... 3
1.1.2 Formulación del Problema ... 3
1.1.3 Sistematización del Problema ... 4
1.1.4 Objetivo General ... 4
1.1.5 Objetivos Específicos ... 4
1.1.6 Justificaciones ... 5
1.2 MARCO TEÓRICO ... 6
1.2.1 Estado del Arte ... 7
1.2.2 Adopción de una Perspectiva Teórica ... 15
1.2.3 Marco Conceptual ... 16
1.2.4 Hipótesis ... 17
CAPÍTULO II ... 18
2.1 ANÁLISIS Y COMPARACIÓN DE ESTÁNDARES INTERNACIONALES Y/O MARCOS DE TRABAJO/MEJORES PRÁCTICAS ... 18
2.1.1 VAL IT ... 18
2.1.2 RISK IT ... 28
2.1.3 COSO ... 35
2.1.4 ITIL ... 41
2.1.5 ISSAI (International Standards of Supreme Audit Institutions) ... 51
2.1.6 ISO 27002 ... 56

2.2 RESUMEN ANÁLISIS DE ESTÁNDARES INTERNACIONALES, MARCOS DE TRABAJO Y MEJORES PRÁCTICAS 70

CAPÍTULO III 71

PROPUESTA DE NORMATIVA BASADA EN COBIT, PARA EL CONTROL INTERNO DE TECNOLOGÍAS DE LA INFORMACIÓN 71

3.1 Evaluar, Orientar y Supervisar (EOS) 72

3.1.1 EOS01 Establecer y mantener el marco de Gobierno 72

3.1.2 EOS02 Aseverar la Entrega de Beneficios 74

3.1.3 EOS03 Asegurar la Optimización del Riesgo 75

3.1.4 EOS04 Asegurar la Optimización de los Recursos 76

3.1.5 EOS05 Asegurar la Transparencia hacia las partes interesadas 77

3.2 Alinear, Planificar y Organizar (APO) 78

3.2.1 APO01 Administrar el marco de gobierno de TI 78

3.2.2 APO02 Administrar la estrategia 81

3.2.3 APO03 Administrar la arquitectura de la entidad 83

3.2.4 APO04 Administrar la innovación 85

3.2.5 APO05 Administrar el portafolio 87

3.2.6 APO06 Administrar los recursos humanos 89

3.2.7 APO07 Administrar los acuerdos de servicio 91

3.2.8 APO08 Administrar los proveedores 93

3.2.9 APO09 Administrar la calidad 94

3.2.10 APO10 Administrar el riesgo 95

3.2.11 APO11 Administrar la seguridad 97

3.3 Construcción, Adquisición e Implementación (CAI) 99

3.3.1 CAI01 Administrar Programas y Proyectos 99

3.3.2 CAI02 Administrar la definición de requisitos 103

3.3.3 CAI03 Administrar la identificación y construcción de soluciones 104

3.3.4 CAI04 Administrar la disponibilidad y la capacidad 107

3.3.5 CAI05 Administrar cambios organizativos 108

3.3.6 CAI06 Administrar los cambios 110

3.3.7 CAI07 Administrar la aceptación del cambio y la evolución 110

3.3.8 CAI08 Administrar el conocimiento 112

3.3.9 CAI09 Administrar los activos 113

3.3.9 CAI10 Administrar la configuración 115

3.4 Entrega, Servicio y Soporte (ESS) 116

3.4.1 ESS01 Administrar Operaciones 116

3.4.2 ESS02 Administrar Peticiones e Incidentes de Servicio 119
3.4.3 ESS03 Administrar los Problemas 121
3.4.4 ESS04 Administrar la Continuidad 123
3.4.5 ESS05 Administrar Servicios de Seguridad 126
3.4.6 ESS06 Administrar Controles de los Procesos del Negocio 130
3.5 Supervisar, Evaluar y Valorar (SEV) 132
3.5.1 SEV01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad 132
3.5.2 SEV02 Supervisar, Evaluar y Valorar el sistema de Control Interno 133
3.5.3 SEV03 Supervisar, Evaluar y Valorar la Conformidad con los Req. Externos 136
3.6 RESUMEN CONTENIDO NORMATIVA PROPUESTA 138
CAPÍTULO IV 141
CONCLUSIONES Y RECOMENDACIONES 141
4.1 Conclusiones 141
4.2 Recomendaciones 142
Bibliografía 144

ÍNDICE DE FIGURAS

Figura 1. Principios, procesos y prácticas de VAL IT 19
Figura 2.Dominios y procesos de VAL IT 21
Figura 3. Prácticas claves de Gestión 22
Figura 4.Objetivos, entradas y salidas de los Dominios de VAL IT 23
Figura 5. Ambitos de Risk IT 29
Figura 6. Relación Objetivos y Componentes 38
Figura 7 Fases del ciclo de vida del servicio 42
Figura 8 Mapa de procesos ITIL 47
Figura 9 Perspectiva COBIT vs ITIL 47
Figura 10. Revisión de seguridad ISSAIs 54
Figura 11. ISO 27002 57
Figura 12. Evolución de COBIT 64
Figura 13. Principios de COBIT 65
Figura 14. Áreas Clave de Gobierno y Gestión de COBIT 5 67
Figura 15. Procesos de Gobierno de TI Empresaria 68
Figura 16. Modelo de Referencia 69
Figura 17. Procesos comunes 69

ÍNDICE DE TABLAS

Tabla 1: Práctica VG1.1 de VAL IT vs proceso EDM01.01 de COBIT 5.....23
Tabla 2: Asociación de controles VAL IT y COBIT 5.....24
Tabla 3: Actividades de los procesos de RISK IT.....30
Tabla 4: Asociación de RG1.1 de Risk IT vs EDM03.01 de COBIT 5.....33
Tabla 5: Asociación de RISK IT y COBIT.....33
Tabla 6: Asociación de RG1.1 de COSO vs EDM03.01 de COBIT 5.....39
Tabla 7: Asociación de COSO y COBIT.....40
Tabla 8: Actividades de las fases de ITIL.....43
Tabla 9: Asociación de la fase de Gestión del servicio de ITIL vs APO02 de COBIT 5.....48
Tabla 10: Asociación de Controles ITIL y COBIT 5.....48
Tabla 11: Asociación Administración de la seguridad de ISSAI vs APO13 y DSS05 de COBIT 5.....55
Tabla 12: Alineación ISSAIs y COBIT 5.....55
Tabla 13: Asociación del control 6.1.1 de ISO/IEC 27002:2013 vs APO01 y APO02 de COBIT 5.....60
Tabla 14: Alineación de ISO 27002:2013 y COBIT 5.....61
Tabla 15: Estándares internacionales, marcos de trabajo y mejores prácticas.....70
Tabla 16: Controles contenidos en normativa propuesta.....138

Resumen

El grupo 410 TECNOLOGÍA DE LA INFORMACIÓN de las Normas de Control Interno de Contraloría General del Estado vigentes desde 2009 cuentan con 17 capítulos que detallan controles a ser aplicados por las áreas de TI de las entidades del sector público Ecuatoriano, controles que por casi una década no han sido actualizados, lo que ha ocasionado que se mantenga una perspectiva de controles no alineados a los avances tecnológicos generados durante los últimos años, en tal razón se realizó una comparación de esta normativa frente a los marcos de referencia internacionales y mejores prácticas obteniendo el diseño de una "***propuesta de normativa basada en COBIT para el control interno de tecnologías de la información del sector público ecuatoriano***" en la que se evidenciaron los vacíos legales existentes en la Norma antes citada; vacíos que ocasionan que no exista una base legal de cumplimiento obligatorio con la que se puedan establecer recomendaciones de prevención, corrección y mejora en todas las entidades del sector público y personas jurídicas que dispongan de recursos públicos que regulen las áreas de Tecnología de la Información poniendo en riesgo la confidencialidad, integridad y disponibilidad de la información, así como a los servicios tecnológicos provistos por TI. Con esta propuesta se plantea evitar y controlar el acceso físico no autorizado, intromisiones en las instalaciones y a la información, asegurar la operación correcta y segura de los recursos de información y finalmente controlar los accesos físicos y lógicos a la información y la infraestructura tecnológica de las entidades del sector público Ecuatoriano.

Palabras clave: control interno, marcos de referencia, controles tecnológicos, sector público

Abstract

The group 410 INFORMATION TECHNOLOGY from the Internal Control Standards of the General Comptroller of the State (CGE) current since 2009 has 17 chapters that detail controls will be applied by IT areas in Ecuadorian public entities, controls that for almost a decade have not been updated, which has caused a perspective of not aligned controls to the technological advances generated during the last years, in such a ratio to this norm was made against the international reference frameworks and best practices obtaining the design of a "***proposed regulation based on COBIT for the internal control of information technologies of Ecuadorian public sector***" in which the legal gaps existing in the aforementioned Standard were evidenced; gaps that cause the absence of legal basis for mandatory compliance in which recommendations for prevention, correction and improvement can be established in all public and legal entities that have public resources that regulate areas of Information Technology involving a risk of confidentiality, integrity and availability of the information, as well as the technological services provided by IT. This proposal sets to avoid and control unauthorized physical access, intrusion into facilities and information, ensure the correct and safe operation of information resources and finally control of physical and logical access to information and the technological infrastructure of the Ecuadorian entities of public sector.

Keywords: internal controls, framework, technological controls, public sector

CAPÍTULO I

INTRODUCCIÓN

1.1 PROBLEMA DE LA INVESTIGACIÓN

1.1.1 Planteamiento del Problema

1.1.1.1 Diagnóstico

Las Normas de Control Interno, vigentes y expedidas mediante acuerdo 039 CG de 16 de noviembre de 2009 y publicadas en el Registro Oficial 78 de 1 de diciembre de 2009, tienen por objeto propiciar con su aplicación, el mejoramiento de los sistemas de control interno y la gestión pública, en relación a la utilización de los recursos estatales y la consecución de los objetivos institucionales. Constituyen el marco que regula y garantiza las acciones de titulares, servidoras y servidores de cada entidad u organismo según su competencia y en función de la naturaleza jurídica de la entidad para que desarrollen, expidan y apliquen los controles internos que provean una seguridad razonable en salvaguarda de su patrimonio. (Pólit, 2009, p.1)

Las Normas de Control Interno contienen el grupo 410 TECNOLOGÍA DE LA INFORMACIÓN el cual detalla 17 capítulos de controles orientados a regular las áreas de Tecnología de la Información que deben ser aplicados en las entidades del sector público y personas jurídicas que dispongan de recursos públicos, a las que se refiere el artículo 225 de la Constitución de la República del Ecuador.

El grupo 410 TECNOLOGÍA DE LA INFORMACIÓN de las Normas de Control Interno se han aplicado durante casi una década sin haber sido actualizadas o mejoradas, lo que ha ocasionado que se mantenga una perspectiva de controles no alineados a los avances tecnológicos generados durante los últimos años, provocando que existan vacíos legales en la normativa vigente impidiendo controlar las vulnerabilidades de los recursos de Tecnología de la Información y Comunicaciones y poniendo en riesgo la información de las entidades ecuatorianas del público.

La falta de actualización en los controles del grupo 410 TECNOLOGÍA DE LA INFORMACIÓN de las Normas de Control Interno ocasiona que no exista una base legal de cumplimiento obligatorio con la que se puedan establecer recomendaciones de prevención, corrección y mejora en todas las entidades, y organismos del sector público ecuatoriano, ya que no se han identificado los vacíos legales existentes en el grupo 410 TECNOLOGÍAS DE LA INFORMACIÓN de las Normas de Control Interno referentes a políticas de control y administración de accesos de los usuarios, control de accesos a las redes y servicios asociados, uso de información confidencial para la autenticación, procedimientos seguros de inicio de sesión, gestión de contraseñas de usuarios, gestión de claves, seguridad del cableado, salida de equipos fuera de las instalaciones de las entidades, gestión de las vulnerabilidades técnicas, mecanismos de seguridad asociados a servicios de red, segregación de redes, política de desarrollo seguro de software, protección de los datos utilizados en pruebas, notificación de los eventos de seguridad, respuesta a los incidentes de seguridad, recopilación de evidencias, regulación de los controles criptográficos entre otros de manera obligatoria.

1.1.1.2 Pronóstico

En caso de no implementar una normativa de cumplimiento obligatorio que llene los vacíos legales existentes en el grupo 410 TECNOLOGÍAS DE LA INFORMACIÓN de las Normas de Control Interno, se pone en riesgo la confidencialidad, integridad y disponibilidad de la información, así como de los servicios tecnológicos provistos por las unidades/áreas/gerencias de Tecnología de la Información.

1.1.1.3 Control de Pronóstico

Identificar los vacíos legales existentes en el grupo 410 TECNOLOGÍA DE LA INFORMACIÓN de las Normas de Control Interno, permitirá incorporar controles, para que todas las entidades del sector público y personas jurídicas que dispongan de recursos públicos regulen las áreas de Tecnología de la Información y mejoren el aseguramiento de la confidencialidad, integridad y disponibilidad de la información, así como de los servicios tecnológicos provistos por las unidades/áreas/gerencias de Tecnología de la Información, evitando de esta manera el acceso físico no autorizado, intromisiones en las instalaciones y a la información, además de asegurar la operación correcta y segura de los recursos de información y finalmente controlar los accesos físicos y lógicos a la información y la infraestructura tecnológica de las entidades, y organismos del sector público Ecuatoriano.

1.1.2 Formulación del Problema

La falta de identificación de vacíos legales en las Normas de Control Interno del grupo 410 "TECNOLOGÍA DE LA INFORMACIÓN", para el sector público ecuatoriano, pone en riesgo la confidencialidad, integridad y disponibilidad de la información y la prestación de servicios en las entidades del estado.

1.1.3 Sistematización del Problema

¿Cuáles son los estándares internacionales relacionados a controles tecnológicos que permiten asegurar la confidencialidad, integridad y disponibilidad de la información?

¿Cuál será el mecanismo de análisis de los estándares internacionales y de las mejores prácticas sobre controles tecnológicos que permiten asegurar las propiedades de la información y la prestación de servicios con el fin de obtener los más aplicables en las entidades públicas?

¿De qué manera se obtendrán controles tecnológicos que permiten asegurar la confidencialidad, integridad y disponibilidad de la información y la prestación de servicios en las entidades del sector público?

1.1.4 Objetivo General

Diseñar una propuesta de Normativa basada en Cobit, para el Control Interno de Tecnologías de la Información del sector Público Ecuatoriano.

1.1.5 Objetivos Específicos

- Identificar los estándares internacionales y las mejores prácticas relacionados a controles tecnológicos que permitan asegurar la confidencialidad, integridad y disponibilidad de la información, y la prestación de servicios a través del compendio de información.
- Analizar los estándares internacionales y las mejores prácticas identificadas, mediante una comparación con COBIT 5 para el desarrollo de los controles idóneos y aplicables a las entidades públicas.
- Diseñar los controles de la Normativa de Control Interno basados en el análisis comparativo realizado con COBIT 5 para asegurar la confidencialidad, integridad

y disponibilidad de la información y la prestación de servicios en las entidades del sector público.

1.1.6 Justificaciones

Desarrollar los controles tecnológicos necesarios para cubrir los vacíos legales de la normativa actual vigente de control interno de las instituciones públicas del Ecuador permitirá asegurar la integridad, confidencialidad y disponibilidad de su información.

Metodológicamente se utilizará como punto de partida los dominios de COBIT 5, debido a que es un marco de referencia para el gobierno de TI, conformado por estándares, herramientas, técnicas y mejores prácticas probadas y aceptadas internacionalmente, que permiten el uso adecuado de TI, comunicación de resultados y el cumplimiento de las metas y objetivos del negocio.

En el documento de investigación "*Propuesta de cumplimiento al artículo 410 de la Norma de Control Gubernamental Moderno emitida en el año 2009 por la Contraloría General del Estado del Ecuador sobre las tecnologías de la información y comunicaciones, aplicando estándares y buenas prácticas internacionales actuales*", propone: una metodología para la gestión de servicios tecnológicos de las entidades del sector público Ecuatoriano, que se alinea con el objetivo de identificar las deficiencias en el marco legal vigente, basado en COBIT 5 ya que es una norma integral y ayuda a las empresas a crear valor a partir de las tecnologías de la información y comunicaciones (Páliz, 2017).; es por esto que se tomará como referente para el desarrollo de la presente propuesta.

La Contraloría General del Estado cuenta con la Dirección Nacional Técnica Normativa, que es la encargada de analizar y emitir nuevos lineamientos, procedimientos,

acuerdos y normas que regirán a las entidades que pertenecen al Estado; siendo un gran aporte para esta Unidad, tener identificado los vacíos legales existentes en el grupo 410 TECNOLOGÍAS DE LA INFORMACIÓN de las Normas de Control Interno para su actualización basada en un estudio, sustentado en un marco de referencia internacional.

1.2 MARCO TEÓRICO

En las organizaciones COBIT es usado para crear un valor óptimo con base en las tecnologías de la información y comunicaciones, manteniendo un equilibrio entre beneficios, optimización de los niveles de riesgo y la utilización de los recursos.

(ISACA, 2012a) señala que COBIT 5 permite que las tecnologías de la información se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad, funcionales y de negocios, considerando los intereses relacionados con las TI de las partes interesadas internas y externas.

Los principios de COBIT 5: satisfacer necesidades de los interesados, cubrir la Organización de una forma integral, aplicar un solo marco integrado, facultar un enfoque holístico y separar el Gobierno de la Administración. Los habilitadores de COBIT 5: principios políticas y marcos; procesos; estructuras organizacionales; cultura, ética y comportamiento; información; servicios, infraestructura y aplicaciones y personas, habilidades y competencias (ISACA, 2012a).; "son genéricos y útiles para las Organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o en el sector público". (ISACA, 2012a, p.6)

1.2.1 Estado del Arte

El Ecuador es un Estado constitucional que se gobierna de manera descentralizada y se encuentra formado por la Función Ejecutiva, la cual está delegada al Presidente de la República y a los Ministros de Estado; la Función Legislativa, que corresponde a la Asamblea Nacional; la Función Judicial, formada por la Corte Nacional de Justicia, el Tribunal Constitucional y Cortes Provinciales; la Función Electoral que se encarga de los procesos electorales y la Función de Transparencia y Control Social, que promueve el control de las entidades y organismos del sector público.

Las entidades del Estado cuentan con una estructura orgánica en la que se incluye un área que gestiona las Tecnologías de Información y Comunicaciones para apoyar el cumplimiento de los objetivos institucionales, área que debe cumplir con los 17 capítulos de controles orientados a regular las áreas de Tecnología de la Información que componen el grupo 410 TECNOLOGÍA DE LA INFORMACIÓN de las Normas de Control Interno de la Contraloría General del Estado.

La seguridad informática es parte de la seguridad de la información, y se enfoca en la protección de la infraestructura tecnológica, incluyendo la información obtenida, su finalidad es asegurar que los recursos del sistema de información de una organización sean empleados de forma correcta, de acuerdo a las políticas establecidas, y que el acceso a la información, así como su modificación, sólo sea permitida a las personas autorizadas.

Víctor Páliz, Magister en Informática, Especialista en Gestión de las Comunicaciones y Tecnologías de la Información, Magister en Gestión de las Comunicaciones y Tecnologías de la Información y Máster en Gestión Pública, en el año 2017, mencionó en su Tesis "*Propuesta de cumplimiento al artículo 410 de la Norma de Control Gubernamental Moderno emitida en el año 2009 por la Contraloría General del*

Estado del Ecuador sobre las tecnologías de la información y comunicaciones, aplicando estándares y buenas prácticas internacionales actuales", que el contenido del grupo 410 TECNOLOGÍA DE LA INFORMACIÓN de las Normas de Control Interno de la Contraloría General del Estado, es básico e incompleto para manejar operativamente el área de tecnología y representa el punto mínimo a cumplir en la gestión del área de tecnología de la información; debido a que no cuenta con requisitos para otorgar mejores servicios de tecnología de la información y comunicaciones, tales como: el análisis de los costos de los servicios, estrategias para brindar un mejor servicio, comunicación a los usuarios, innovación y desarrollo; brindando un aporte deficiente en los servicios públicos y en los procesos institucionales. (Páliz, 2017)

William Villacís, Magister en Evaluación y Auditoria de Sistemas Tecnológicos, en el año 2014, señaló en su trabajo de investigación "*Guía de evaluación de la Gestión de TI con aplicación de COBIT y COSO en el sector público*", que la aplicación de los procesos de COBIT, dependen en la actualidad de la voluntad y el grado de madurez que necesita la entidad pública, teniendo que relacionar los dominios y procesos de COBIT con las Normas de Control Interno incumplidas para tomar acciones correctivas posterior a la emisión del Informe de Auditoría aprobado por la Contraloría General del Estado. (Villacís, 2014)

López Cabrera Sandra Elizabeth, Molina Ventura José Raúl y Quintanilla Quintanilla Flor de María, en el año 2008, mencionaron en su Trabajo de Investigación "*Procedimientos de auditoria aplicados a los sistemas de información computarizados para la detección, prevención y corrección de delitos informáticos*", no existe una Base Técnica local que sirva de forma específica para auditar los sistemas de información computarizados de las empresas; para tal efecto, se considerarán en lo que sean aplicables

los objetivos de control recomendados por COBIT, con el fin de desarrollar procedimientos de auditoria que se apliquen a los sistemas de información y que sirvan de guía para la detección, prevención y posible corrección de delitos informáticos (López, Molina y Quintanilla, 2008).

Finalmente, "COBIT 5 … es la norma a seguir debido a que es integral y ayuda a las empresas a crear valor a partir de las tecnologías de la información y comunicaciones" (Páliz, 2017, p.v). y representa una norma integral para el gobierno y la gestión de tecnologías de la información que cubre los procesos más importantes del área, tales como: seguridades, gestión de servicio, gobierno, arquitectura empresarial y desarrollo de sistemas.

Para alcanzar el objetivo de diseñar una propuesta de Normativa basada en Cobit, para el Control Interno de Tecnologías de la Información del sector Público Ecuatoriano se deben analizar Estándares y Marcos de Referencia reconocidos a nivel mundial.

Marcos de Referencia Internacionales

La ISO (Organización Internacional para Estandarización) e IEC (Comisión Internacional Electrotécnica forman el sistema especializado para estandarización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de Estándares Internacionales a través de los comités técnicos establecidos por la respectiva organización para tratar campos particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales conjuntamente con ISO e IEC, también toman parte en el trabajo. En el campo de tecnologías de información, ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1. (Norma Técnica Ecuatoriana 27002:2009, 2008)

ISO/IEC 27002

El estándar internacional fue publicado por la ISO (www.iso.org/ISO/home.htm) y la IEC, que establecieron el comité técnico mixto ISO/IEC JTC 1. La fuente histórica para el estándar fue BS 7799-1, cuyas partes esenciales fueron tomadas en el desarrollo de la norma ISO/IEC 17799:2005 Tecnología de la Información – Código de Prácticas para la Gestión de Seguridad de la Información. Fue desarrollado y publicado por la British Standards Institution (BSI), denominado como BS 7799-1:1999. (Hardy, 2008, p.17)

La norma publicó su primera edición en el año 2000 y actualizada en junio de 2005. Se puede clasificar como las mejores prácticas actuales en materia de sistemas de gestión de seguridad de la información. La BS 7799 original fue revisada y reeditada en septiembre de 2002. (Hardy, 2008, p.17)

La ISO 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información, por esta razón es el primer paso a seguir en la protección de la información. (Molina, Rodríguez, Sánchez y Vergel, 2012)

El objetivo de ISO/IEC 27002:2005 es brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión para mejorar la fiabilidad en la seguridad de la información en las relaciones interorganizacionales. Aquí se definen las estrategias de 133 controles de seguridad organizados bajo 11 dominios. (Hardy, 2008, p.17)

COBIT

Es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse de que se ajusta de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales. COBIT brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas. (Hardy, 2008)

Debido a que COBIT es un conjunto de herramientas y técnicas probadas y aceptadas internacionalmente, su implementación es una señal de buena gestión en una organización. Ayuda a los profesionales de TI y a usuarios de empresas a demostrar su competencia profesional a la alta dirección. Como ocurre con muchos procesos de negocio genéricos, existen estándares y mejores prácticas de la industria de TI que las empresas deberían seguir cuando utilizan las TI. COBIT se nutre de estas normas y proporciona un marco para implementarlas y gestionarlas. (Hardy, 2008)

ITIL

Las organizaciones dependen de las TI para satisfacer sus objetivos corporativos, necesidades de negocios y entregar valor a sus clientes para que esto ocurra de una forma gestionada, responsable y repetible, la empresa debe asegurar que los servicios recibidos de alta calidad de TI deben:

- Satisfacer las necesidades de la empresa y los requisitos de los usuarios.
- Cumplir con la legislación.
- Asignarse y entregarse de forma eficaz y eficiente.
- Revisarse y mejorarse de forma continua. (Hardy, 2008)

La gestión de servicios de TI se refiere a la planificación, aprovisionamiento, diseño, implementación, operación, apoyo y mejora de los servicios de TI que sean apropiados a las necesidades del negocio. ITIL proporciona un marco de trabajo de mejores prácticas integrales, consistente y coherente para la gestión de servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de Tecnología. (Hardy, 2008)

COSO

Es un marco de referencia para la implementación, gestión y control de un adecuado Sistema de Control Interno cuya misión es proveer directivas mediante el desarrollo de marcos de trabajo comprensibles y lineamientos en gestión de riesgo empresarial, control interno y disuasión del fraude designado para mejorar el rendimiento organizacional y de gobierno y reducir el alcance del fraude en las organizaciones. (The Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017)

El marco de COSO 2013 mantiene la definición de Control Interno y los cinco componentes del mismo, pero incluye mejoras y aclaraciones con el objetivo de facilitar el uso y su aplicación en las entidades.

Es importante considerar que el Control Interno es un proceso dinámico, iterativo e integral. Por lo tanto, el Control Interno no es un proceso lineal en el que uno de los componentes afecta solo al siguiente. Más bien es un proceso integrado en el que los componentes pueden y van a impactar en cualquier otro. (Galaz, Yamazaki y Ruiz, 2015)

RISK IT

Es un marco basado en un conjunto de principios y guías, procesos de negocio y directrices de gestión que se ajustan a estos principios. (ISACA, 2009b)

El marco de los riesgos de TI, RISK IT, se complementa con COBIT, que proporciona un marco integral para el control y la gestión de las organizaciones de soluciones y servicios de TI. Aunque COBIT establece las mejores prácticas para la gestión de riesgos proporcionando un conjunto de controles para mitigar los riesgos de TI, RISK IT establece las mejores prácticas con el fin de establecer un marco para las organizaciones para identificar, gobernar y administrar los riesgos asociados a su negocio. (ISACA, 2009a) Es utilizado para ayudar a implementar el gobierno de TI, y las organizaciones que han adoptado o piensan adoptar COBIT como marco de su gobierno de TI pueden utilizar RISK IT para mejorar la gestión de sus riesgos.

COBIT, propiedad de ISACA, se encarga de gestionar todas las actividades relacionadas con TI en la organización. Estos procesos tienen que tratar con eventos internos o externos a la organización. Los eventos internos pueden incluir los incidentes operacionales, los fracasos del proyecto, cambios de la estrategia de TI y las fusiones. Los eventos externos pueden incluir cambios en las condiciones del mercado, nuevos competidores, nuevas tecnologías disponibles y las nuevas regulaciones que le afectan (ISACA, 2009a, p.7).

"Estos eventos, plantean un riesgo y una oportunidad para evaluar el mismo y generar las soluciones oportunas. La dimensión del riesgo, y cómo gestionarlo, es el tema principal de RISK IT" (ISACA, 2009a, p.7).

RISK IT es el riesgo comercial, es decir, el riesgo de los negocios asociados con el uso, la propiedad, la operación, la participación, la influencia y la adopción de las TI

dentro de una organización. Se compone de eventos relacionados con TI que podrían afectar a la organización. Esto incluye tanto la frecuencia y la magnitud incierta, la creación de problemas en el cumplimiento de metas y objetivos estratégicos, así como la incertidumbre en la búsqueda de oportunidades (ISACA, 2009a, p.11).

VAL IT

Es un marco de referencia de gobierno que incluye principios rectores generalmente aceptados y procesos de soporte relativos a la evaluación y selección de inversiones de negocios de TI. (ISACA, 2008)

Val IT permite soportar el objetivo de negocio de realizar un valor óptimo de las inversiones de negocio en TI a un costo económico y con un nivel aceptable de riesgo y está guiado por un conjunto de principios aplicados a procesos de gestión de valor que son impulsados por prácticas claves de gestión con referencias cruzadas a los controles claves de COBIT y que se miden por Métricas de resultados y rendimiento.

Para obtener la rentabilidad de la inversión, los socios de las inversiones posibilitadas por TI deberán aplicar los principios de Val IT a los procesos de Gobierno de valor, Gestión de cartera y Gestión de Inversiones.

En Val IT, se facilitan guías para maximizar la calidad de los casos de negocio, poniendo especial énfasis en la definición de indicadores claves, tanto financieros (valor neto actual, tasa interna de rentabilidad y período de recuperación) como no financieros, y en la evaluación y valoración global del riesgo de pérdidas.

OLACEFS

La Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (OLACEFS) es un organismo internacional, autónomo, independiente y apolítico, creado como una asociación de carácter permanente que se encarga de cumplir

funciones de investigación científica especializada y desarrollar tareas de estudio, capacitación, especialización, asesoría y asistencia técnica, formación y coordinación al servicio de sus miembros. (Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores [OLACEFS], 2012)

La Estrategia 3: Tecnología de Información y Comunicación, del Plan Estratégico para los años 2011 al 2015, señala: "*Desarrollar y promover un estándar tecnológico para la Organización y las EFS de la Región, que le permita contar con una página Web dotada de un conjunto de servicios interactivos al servicio de los miembros de la Organización (foros, videoconferencias, biblioteca virtual, multilenguaje, manejo de roles y usuarios, sistemas de entornos de aprendizaje virtual, etc.)".* (OLACEFS, 2015)

ISO / IEC 27001 establece los requisitos normativos para el desarrollo y operación de un SGSI, incluyendo un conjunto de controles para el control y la mitigación de los riesgos asociados con la Información que la organización busca proteger mediante la operación de su SGSI, (International Standarization Organization, 2014) y además la norma ISO 27001 cubre a todo tipo de organizaciones (empresas comerciales, agencias, gubernamentales, organizaciones sin ánimo de lucro) e independientemente de su tamaño (pequeña, mediana o gran empresa), tipo o naturaleza.

1.2.2 Adopción de una Perspectiva Teórica

En base a lo analizado en el estado del arte, de forma particular en los trabajos que son mencionados a continuación:

Páliz (2017) en su investigación "*Propuesta de cumplimiento al artículo 410 de la Norma de Control Gubernamental Moderno emitida en el año 2009 por la Contraloría General del Estado del Ecuador sobre las tecnologías de la información y comunicaciones, aplicando estándares y buenas prácticas internacionales actuales*",

señala el análisis de buenas prácticas como ITIL, PMBOK y COBIT 5 para crear la propuesta de mejora; también Villacís (2014) en su trabajo "*Guía de evaluación de la Gestión de TI con aplicación de COBIT y COSO en el sector público*" indica que COBIT es un referente para las mejora de las Normas de Control Interno; y, López, Molina y Quintanilla (2008) en su documento "*Procedimientos de auditoría aplicados a los sistemas de información computarizados para la detección, prevención y corrección de delitos informáticos*" menciona que los objetivos de control recomendados por COBIT sirven de guía para la detección, prevención y posible corrección de los delitos informáticos; por lo tanto, una vez analizados los tres documentos antes citados, consideramos que la perspectiva teórica de los tres autores coinciden en que COBIT es un marco de referencia completo y que se encuentra orientado a cumplir con el objetivo de asegurar la confidencialidad, disponibilidad e integridad de la información que se encuentra en riesgo por la falta de identificación de vacíos legales en la normativa legal vigente que rige a las entidades del sector público Ecuatoriano.

Es así, que este trabajo de investigación desarrollará la propuesta de controles para solventar los vacíos legales existentes tomando como base el Marco de Referencia COBIT 5, como señalan los autores mencionados previamente, este es un marco completo y adaptable a cualquier tipo de entidad.

1.2.3 Marco Conceptual

Confidencialidad

Propiedad de la información mediante la cual el acceso a la misma se brinda únicamente mediante una autorización y de forma controlada.

Se refiere a la protección de información sensitiva contra revelación no autorizada. (ISACA, 2012b)

Integridad

Propiedad de la información mediante la cual se mantiene sin cambios en el tiempo.

Está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio. (ISACA, 2012b)

Si la información tiene integridad, entonces está completa y libre de errores. (ISACA, 2012b)

Disponibilidad

Es el acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (Neira & Spohr, 2010)

Disponibilidad es una de las metas de la calidad de la información que están bajo los encabezados de accesibilidad y seguridad. (ISACA, 2012b)

1.2.4 Hipótesis

La identificación de vacíos legales en las Normas de Control Interno del grupo 410 TECNOLOGÍA DE LA INFORMACIÓN, permitirá diseñar una propuesta de normativa basada en COBIT 5, que permita brindar confidencialidad, integridad y disponibilidad de la información y la prestación de servicios en las entidades del sector público ecuatoriano.

CAPÍTULO II

2.1 ANÁLISIS Y COMPARACIÓN DE ESTÁNDARES INTERNACIONALES Y/O MARCOS DE TRABAJO/MEJORES PRÁCTICAS

En lo referente a Estándares Internacionales y Marcos de Referencia se pueden encontrar un sin número de alternativas sobre las Tecnologías de la Información; sin embargo, al tratarse de una propuesta de Normativa de Control Interno, ~~s~~ para las entidades públicas del sector Ecuatoriano, se deben analizar las que contengan controles que sean aplicables a esa realidad.

En este caso se analizarán los marcos de referencia Val IT, Risk IT, COBIT 5, COSO e ITIL; así como las Normas Internacionales ISO e ISSAI, para la elaboración de la propuesta de Normativa de Control Interno de manera que contenga un compendio de la mayor cantidad de controles actuales e idóneos a la realidad ecuatoriana y que sean aplicadas en las entidades del sector público.

2.1.1 VAL IT

ISACA en el 2008 mencionó que VAL IT es un marco creado por el IT Governance Institute (ITGI) que mediante guías, procesos y prácticas de soporte ayuda a las empresas a optimizar las inversiones realizadas en tecnología con un valor razonable y un nivel de riesgo aceptable; y está diseñado para alinearse con COBIT.

Dentro de VAL IT existen principios, procesos y prácticas que están conectados entre sí, y apalancan la creación de un valor óptimo sobre las inversiones autorizadas de TI, el que es un objetivo empresarial. Inicialmente se encuentran los principios que son aplicados en los procesos

de la administración del valor, mismos que son aprobados por prácticas administrativas claves y éstos a su vez son medidos a través del rendimiento de objetivos y métricas. (ISACA, 2008)

Figura 1. Principios, procesos y prácticas de VAL IT
Fuente: ISACA, VAL IT Framework (ISACA, 2006)

ISACA (2006) mencionó los principios básicos, dominios y procesos de VAL IT, siendo éstos los siguientes:

Los principios básicos son 7:

1. Las inversiones de TI autorizadas serán administradas como un portafolio de inversiones.
2. Las inversiones de TI autorizadas incluirán el ámbito completo de actividades que se requieran alcanzar para darle valor al negocio.
3. Las inversiones de TI autorizadas serán administradas a través de todo el ciclo de vida económico.
4. Las prácticas de entrega de valores reconocerán que hay diferentes categorías de inversiones que serán evaluadas y administradas de diferente manera.
5. Las prácticas de entrega de valores definirán y monitorearán las métricas claves y responderán rápidamente a cualquier cambio o desviación.
6. Las prácticas de entrega de valores comprometerán a todos los patrocinadores y asignarán la contabilización apropiada para la entrega de capacidades y la realización de los beneficios del negocio.
7. Las prácticas de entrega de valores están en constante monitoreo, evaluación y mejora.

VAL IT comprende 3 Dominios:

- Gobierno de valor (**VG**), busca asegurar que las prácticas de administración de valores de TI se encuentren dentro de la empresa.
- Gestión de cartera (**PM**), tiene como objetivo asegurar que la empresa afirme un valor óptimo para las inversiones de TI durante todo el ciclo de vida económico, alineándose con los objetivos del negocio.
- Gestión de inversiones (**IM**), asegura que las inversiones autorizadas para TI contribuyan de forma óptima.

A su vez, estos dominios cuentan con diferentes procesos que se detallan a continuación:

- Gobierno de valor (VG):
    - Implantar la dirección estratégica que tomarán las inversiones de TI.
    - Definir e implementar procesos.
    - Definir las características de las inversiones que se realizarán en el área de TI.
    - Alinear e integrar la gestión de valor con la planificación financiera empresarial.
    - Establecer el marco de gobierno, monitoreo y control.
    - Mejorar continuamente las prácticas de la gestión del valor.

- Gestión de cartera (PM):
    - Establecer una combinación entre la dirección estratégica y los objetivos de las inversiones.
    - Gestionar la cartera global de la empresa.
    - Establecer y gestionar los perfiles de los recursos.
    - Evaluar, priorizar y seleccionar nuevas inversiones.
    - Monitoreo del rendimiento de la cartera.
    - Definir umbrales para las inversiones.

- Gestión de inversiones (IM):
    - Definir un programa y el caso de negocio detallado con su respectiva documentación.
    - Entender con claridad los posibles programas de inversión.
    - Desarrollar el plan del programa.
    - Gestionar el programa durante todo el ciclo de vida económico.
    - Desarrollar el caso de negocio de forma detallada.
    - Lanzar y gestionar el programa.
    - Actualizar el portafolio de TI.
    - Actualizar el caso de negocio.
    - Monitorear y emitir reportes sobre el programa.
    - Desechar el programa.

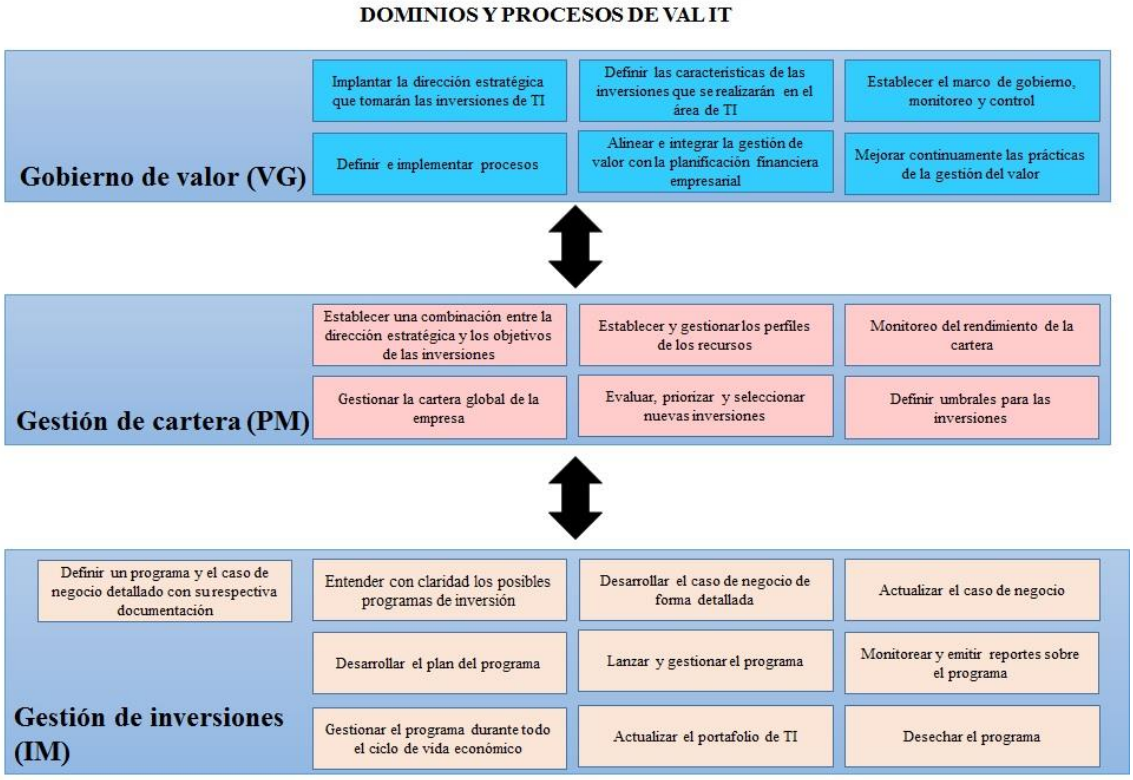

Figura 2.Dominios y procesos de VAL IT
Fuente: ISACA, VAL IT Dominios y Procesos (ISACA, 2008)

ISACA (2006) señala adicionalmente que existen prácticas que ayudan a que la gestión de TI sea adecuada, siendo éstas las siguientes:

Para el proceso de Gobierno de Valor (VG):

VG1. Garantizar liderazgo informado y comprometido
VG2. Definir e implementar procesos
VG3. Definir roles y responsabilidades
VG4. Garantizar responsabilidad apropiada y aceptada
VG5. Definir necesidades de información
VG6. Establecer necesidades de informes
VG7. Establecer estructuras organizativas
VG8. Establecer dirección estratégica
VG9. Definir categorías de inversión
VG10. Determinar un objetivo de composición ('mix') de cartera
VG11. Definir criterios de evaluación por categoría

En el caso de la Gestión de cartera (PM):

PM1. Mantener un inventario de recursos humanos
PM2. Identificar necesidades de recursos
PM3. Realizar un análisis de laguna (gap)
PM4. Desarrollar un plan de asignación de recursos

PM5. Monitorizar necesidades y utilización de recursos
PM6. Establecer un umbral de inversión
PM7. Evaluar el caso del negocio del concepto de programa inicial
PM8. Evaluar y asignar una puntuación relativa al caso de negocio del programa
PM9. Crear una visión de la cartera global
PM10. Tomar y comunicar la decisión inversora
PM11. Fijar etapas y financiar los programas seleccionados
PM12. Optimizar rendimiento de la cartera
PM13. Volver a priorizar la cartera
PM14. Monitorizar e informar sobre el rendimiento de cartera

Para la Gestión de inversiones (IM):

IM1. Desarrollar una definición a alto nivel de la oportunidad de inversión
IM2. Desarrollar un caso de negocio del concepto de programa inicial
IM3. Adquirir un claro entendimiento de los programas candidatos
IM4. Realizar análisis de alternativas
IM5. Desarrollar un plan de programas
IM6. Desarrollar un plan de realización de beneficios
IM7. Identificar costes y beneficios de todo el ciclo de vida
IM8. Desarrollar una situación de negocio detallada del programa
IM9. Asignar claramente la responsabilidad y propiedad
IM10. Iniciar, planear y lanzar programa
IM11. Gestionar el programa
IM12. Gestionar / hacer un seguimiento de los beneficios
IM13. Actualizar el caso de negocio
IM14. Monitorizar e informar sobre el rendimiento del programa
IM15. Retirar el programa (ISACA, 2008)

Figura 3. Prácticas claves de Gestión
Fuente: Prácticas para la Gestión de Procesos Val IT (Espinoza, 2013)

Cada uno de estos dominios tiene su propio objetivo principal, entradas, salidas, métricas de proceso y métricas de dominio, como se puede observar en la figura:

Dominio	Objetivo del Dominio	Entradas	Salidas	Métricas del Proceso	Métricas del Dominio
Gobierno de Valor (VG)	Optimizar el valor de las inversiones de negocio habilitadas por tecnología de una organización.	- Estrategia de negocio - Gobierno empresarial y marco de trabajo de control - Aproximaciones de la inversión empresarial	- Compromiso de la directiva - Requerimientos del gobierno de valor con roles, responsabilidades y cuentas - Características del portafolio y categorías de inversión	- Nivel de acuerdo de la directiva en los principios de gobierno - Nivel de compromiso de la directiva - Grado de implementación y conformidad con el proceso de gestión de la administración	- Maduración del valor de la gestión de procesos
Gestión de cartera (PM)	Asegurar que el portafolio general de inversiones habilitadas por TI, se encuentre alineado con los objetivos estratégicos de la organización y contribuye con un valor óptimo al logro de los mismos	- Estrategia de negocio - Características del portafolio y categorías de inversión - Presupuesto y recursos disponibles - Casos de negocio detallados	- Programas de inversión aprobados - Vistas del portafolio de inversiones general - Reportes de rendimiento del portafolio	- Nivel de satisfacción sobre la contribución de TI sobre el valor de negocio - Porcentaje de desembolsos de TI que tienen una trazabilidad directa con la estrategia del negocio - Porcentaje de incremento en el valor del portafolio en el tiempo	- Porcentaje de estimación opcional del valor, esto asegura las inversiones permitidas para el portafolio de TI empresarial
Gestión de inversiones (IM)	Asegurar que los programas individuales de inversión habilitada por TI, generan un valor óptimo a un costo accesible con un nivel de riesgo conocido y aceptable	- Estrategia de negocio Requerimientos de negocio detallados - Características del portafolio e incorporaciones - Recursos disponibles	- Casos de negocio detallado, incuyendo el ciclo de vida de costos y beneficios - Plan de progarma incluyendo presupuesto y recursos - Reportes de rendimiento de programa - Portafolio de operaciones de TI actualizado	- Número de ideas nuevas para cada categoría de inversión y el porcentaje invertido en cada caso de negocio - Casos de negocio completos y cumplidos (inicialmente y actualizados) - Porcentaje del valor esperado realizado	- Contribución de inversiones individuales de TI para un valor óptimo

Figura 4.Objetivos, entradas y salidas de los Dominios de VAL IT
Fuente: ISACA, Lineamientos de Administración de Alto Nivel(ISACA, 2008)

Controles asociados de VAL IT y COBIT

Después de identificar las prácticas claves que forman parte del marco de referencia Val IT, pueden ser asociadas con los dominios y controles de COBIT 5, según el ámbito de su aplicación; por ejemplo, se puede asociar la práctica clave: "VG1.1 Desarrollar un entendimiento de la relevancia de TI y el papel del Gobierno" de VAL IT con el proceso de "EDM01.01 Evaluar el sistema de gobierno", de COBIT 5 de la siguiente manera:

Tabla 1:

Práctica VG1.1 de VAL IT vs proceso EDM01.01 de COBIT 5

VAL IT	COBIT 5
Desarrollar un entendimiento de la relevancia de TI y el papel del Gobierno Todos los ejecutivos deben conocer sobre los problemas estratégicos de TI, como la dependencia de TI; y el conocimiento y las capacidades tecnológicas, de forma que exista un acuerdo entre TI, las otras unidades de negocio y los ejecutivos respecto al significado actual y potencial de TI para la estrategia empresarial. Los líderes empresariales deben comprender los elementos claves de gobierno que son	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. (ISACA, 2012a)

VAL IT	COBIT 5
requeridos para la entrega segura, confiada y con un costo efectivo del valor óptimo del uso de los servicios, los activos y los recursos de TI, tanto existentes como nuevos. (ISACA, 2006)	

Nota: Elaborada por los autores: Figueroa F, Hinojosa L.

Es decir, el proceso EDM01.01 perteneciente al dominio de COBIT 5 "EDM" puede ser asociado con la práctica clave VG1.1 de VAL IT, ya que ambos tratan sobre la evaluación del Gobierno de TI. Con esta explicación se puede entender la matriz de asociación de controles que se presenta a continuación:

Tabla 2:

Asociación de controles VAL IT y COBIT 5

Prácticas Clave de Gestión en VAL IT 2.0 cubiertas en COBIT	APO01	APO02	APO05	APO06	APO07	BAI01	BAI10	EDM01	EDM02
VG1.1 Desarrollar un entendimiento de la relevancia de TI y el papel del Gobierno								.1	
VG1.2 Establecer líneas de notificación efectivas								.1	
VG1.3 Establecer un foro de liderazgo	.1							.2	
VG1.4 Definir el valor para la compañía									.2
VG1.5 Asegurar el alineamiento e integración de las estrategias de negocio y TI con los objetivos clave del negocio		.1							
VG2.1 Definir el marco de gobierno del valor								.2	
VG2.2 Evaluar la calidad y cobertura de los procesos actuales	.7								
VG2.3 Identificar y priorizar los requisitos de los procesos	.7								
VG2.4 Definir y documentar los procesos	.7								
VG2.5 Establecer, implementar y comunicar los roles, responsabilidades e imputabilidades	.2								

Prácticas Clave de Gestión en VAL IT 2.0 cubiertas en COBIT	APO01	APO02	APO05	APO06	APO07	BAI01	BAI10	EDM01	EDM02
VG2.6 Establecer las estructuras organizativas	.2							.2	
VG3.1 Definir los tipos de portafolios									.2
VG3.2 Definir las Categorías (dentro de los portafolios)									.2
VG3.3 Desarrollar y comunicar el criterio de evaluación (para cada categoría)									.2
VG3.4 Asignar pesos a los criterios									.2
VG3.5 Definir los requerimientos para los umbrales de cada estado y otras revisiones (para cada categoría)									.2
VG4.1 Revisar las prácticas actuales de presupuestación de la empresa				.3					
VG4.2 Determinar los requerimientos para la práctica de planificación de la gestión de valor				.1					
VG4.3 Identificar los cambios requeridos				.1					
VG4.4 Implementar prácticas de planificación financiera óptimas para la gestión de valor				.1					
VG5.1 Identificar las métricas clave									.3
VG5.2 Definir los procesos de captura de información y sus enfoques									.3
VG5.3 Definir los métodos y técnicas de información									.3
VG5.4 Identificar y supervisar las acciones de mejora del rendimiento									.3
VG6.1 Implementar 'lecciones aprendidas'									.3
PM1.1 Revisar y asegurar que la estrategia y objetivos del negocio son claros			.1						
PM1.2 Identificar oportunidades para que TI influya y apoye a la estrategia del negocio			.1						
PM1.3 Definir una diversidad de inversiones apropiada			.1						

Prácticas Clave de Gestión en VAL IT 2.0 cubiertas en COBIT	APO01	APO02	APO05	APO06	APO07	BAI01	BAI10	EDM01	EDM02
PM1.4 Traducir los objetivos y estrategia del negocio en objetivos y estrategia de TI			.1						
PM2.1 Determinar los fondos de inversión en su conjunto			.2						
PM3.1 Crear y mantener un inventario de recursos humanos para el negocio					.1				
PM3.2 Entender la demanda actual y futura (para los recursos humanos del negocio)					.1				
PM3.2 Identificar déficits (entre la demanda actual y futura de los recursos humanos para el negocio)					.1				
PM3.4 Crear y mantener planes tácticos (para los recursos humanos del negocio)					.1				
PM3.5 Supervisar, revisar y ajustar el Personal y su asignación a las funciones del negocio					.5				
PM3.6 Crear y mantener un inventario de recursos humanos de TI					.5				
PM3.7 Entender la demanda actual y futura (para los recursos humanos de TI)					.5				
PM3.8 Identificar déficits (entre la demanda actual y futura de los recursos humanos para TI)					.5				
PM3.9 Crear y mantener planes tácticos (para los recursos humanos de TI)					.5				
PM3.10 Supervisar, revisar y ajustar (el Personal y su asignación a las funciones de TI)					.5				
PM4.1 Evaluar y asignar puntuaciones comparativas a los casos de negocio del programa			.3						
PM4.2 Crear una vista general del listado de inversiones			.3						
PM4.3 Tomar y Comunicar decisiones de inversión			.3						
PM4.4 Especificar los umbrales de estado y asignar fondos a programas seleccionados			.3						

Prácticas Clave de Gestión en VAL IT 2.0 cubiertas en COBIT	APO01	APO02	APO05	APO06	APO07	BAI01	BAI10	EDM01	EDM02
PM4.5 Ajustar los objetivos de negocio, previsiones y presupuestos			.3						
PM5.1 Supervisar e informar sobre el rendimiento del portafolio de inversiones			.4						
PM6.1 Optimizar el rendimiento del portafolio de inversiones			.4						
PM6.2 Repriorizar el portafolio de inversiones			.4						
IM1.1 Reconocer oportunidades de inversión			.3						
IM1.2 Desarrollar el caso de negocio inicial sobre el concepto del programa						.2			
IM1.3 Evaluar el caso de negocio inicial sobre el concepto del programa			.3						
IM2.1 Desarrollar un entendimiento claro y completo del programa candidato						.2			
IM2.2 Realizar el análisis de alternativas						.2			
IM3.1 Desarrollar el plan del programa						.4			
IM4.1 Identificar el ciclo de vida completo de los beneficios y costes						.4			
IM4.2 Desarrollar un plan para la realización de los beneficios						.4			
IM4.3 Realizar las revisiones apropiadas y obtener las validaciones/ aprobaciones						.03 - .04			
IM5.1 Desarrollar el caso de negocio detallado del programa						.2			
IM5.2 Asignar claramente la responsabilidades y la propiedad						.2			
IM5.3 Realizar las revisiones adecuadas y obtener las validaciones / aprobaciones						.02 - .03			
IM6.1 Planificar los proyectos y recursos y lanzar el programa						.5			
IM6.2 Gestionar el programa						.5			
IM6.3 Rastrear y administrar los beneficios						.5			

Prácticas Clave de Gestión en VAL IT 2.0 cubiertas en COBIT	APO01	APO02	APO05	APO06	APO07	BAI01	BAI10	EDM01	EDM02
IM7.1 Actualizar los portafolios de TI operativos			.5						
IM8.1 Actualizar el caso de negocio						.4			
IM9.1 Supervisar e informar sobre el rendimiento del programa (entrega de la solución)						.6			
IM9.2 Supervisar e informar sobre el rendimiento del programa (resultado de beneficios)						.6			
IM9.3 Supervisar e informar sobre el rendimiento del programa (entrega del servicio)						.6			
IM10.1 Cerrar el programa (ISACA, 2006)							.14		

Nota: Las prácticas claves de Gestión en VAL IT 2.0 fueron tomadas de ISACA (2006). Elaborado por los autores: Figueroa F, Hinojosa L.

Al comparar los marcos de trabajo VAL IT y COBIT se observa que van de la mano, inicialmente COBIT tenía un enfoque únicamente en la Tecnologías de la Información; mientras VAL IT se usaba en la gestión del valor de las inversiones de TI; sin embargo, al asociarlos se obtiene un marco que abarca una visión con un enfoque gerencial, con el que se mantiene un negocio más estable y exitoso; que toma en cuenta los objetivos de las Tecnologías de la Información desde un punto de vista de gobierno de TI, con el que se busca obtener beneficios con la gestión del valor de las inversiones en curso de todos los procesos de tecnología y a través de la entrega de soluciones, la implementación de operaciones y la entrega de servicios de TI; administrando el portafolio de inversiones y el rendimiento de las mismas.

2.1.2 RISK IT

Es un marco creado por ISACA, basado en un conjunto de principios y guías, procesos de negocio y directrices de gestión producto de la investigación y aporte de la experiencia conjunta de un equipo global de especialistas, cuya misión fue la de facilitar a la alta Gerencia,

una administración efectiva de los riesgos de TI relacionados con el negocio, a partir de su identificación y evaluación (ISACA, 2009b).

RISK IT se complementa con COBIT, por el control y administración de las organizaciones de soluciones y servicios de TI (ISACA, 2009b).

COBIT define prácticas de gestión de riesgos proveyendo controles para mitigar riesgos de TI, y por su parte RISK IT detalla prácticas para las organizaciones con el objetivo de identificar, gobernar y administrar los riesgos asociados a su negocio (ISACA, 2009b).

Principios

ISACA en el año 2009 describió que Risk IT se basa en 6 principios:

1. Siempre se alinea con los objetivos de la organización.
2. Alinear la gestión de TI con el riesgo organizacional con ERM
3. Balance de los costos y beneficios de la gestión de los riesgos de TI.
4. Promueve la comunicación abierta y justa de los riesgos de TI.
5. Establece la definición y ejecución de las responsabilidades personales para el funcionamiento dentro de los niveles de tolerancia aceptables y bien definidos.
6. Es un proceso continuo y parte de las actividades diarias (ISACA, 2009a).

Ámbitos

Conforme lo indicado por ISACA, "*The Risk IT Framework*" se divide en tres ámbitos: Gobierno del riesgo, Evaluación de riesgos y Respuesta de riesgo, cada uno con tres procesos:

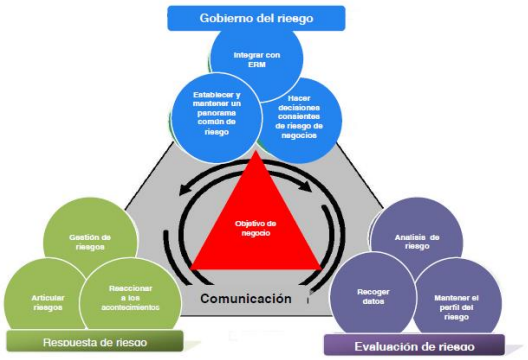

Figura 5. Ambitos de Risk IT
Elaborado por ISACA, Marco de Riesgo de TI (ISACA, 2009a)

1. Gobierno del riesgo (**RG**): Garantiza que las tecnologías de gestión de los riesgos de las prácticas estén arraigadas en la empresa, lo que le permite certificar una óptima rentabilidad ajustada al riesgo.

   - RG1 Establecer y mantener una visión común de riesgo.
   - RG2 Integrar con la gestión de Riesgos de la empresa ERM.
   - RG3 Hacer decisiones conscientes del riesgo del negocio.

2. Evaluación de riesgos (**RE**): Asegura que los riesgos relacionados con IT y las oportunidades son identificados, analizados y presentados en términos de negocio.

   - RE1 Recoger datos.
   - RE2 Analizar los riesgos.
   - RE3 Mantener el perfil de riesgo.

3. Respuesta de riesgos(**RR**): Asegura que las Tecnologías de la Información que están relacionadas con asuntos de riesgos, oportunidades y eventos, se tratan de una manera rentable y en línea con las prioridades del negocio.

   - RR1 Articular el riesgo
   - RR2 Gestión de riesgos
   - RR3 Reaccionar a los eventos (ISACA, 2009a).

Las actividades para cada uno de los procesos del marco de trabajo RISK IT, están conformadas de acuerdo al siguiente detalle:

Tabla 3:

Actividades de los procesos de RISK IT

Proceso	Actividad
RG1	RG1.1 Realizar la evaluación del riesgo en TI de la compañía.
	RG1.2 Proponer los umbrales de tolerancia de riesgo de TI.
	RG1.3 Aprobar la tolerancia al riesgo.
	RG1.4 Alinear la política de riesgos de TI
	RG1.5 Promover una cultura de reconocimiento del riesgo en TI.
	RG1.6 Alentar una comunicación efectiva del riesgo en TI.
RG2	RG2.1 Establecer y mantener la responsabilidad para la gestión del riesgo en TI.
	RG2.2 Coordinar la estrategia del riesgo en TI y del negocio.
	RG2.3 Adaptar las prácticas del riesgo en TI a las prácticas del riesgo en la empresa.
	RG2.4 Proporcionar los recursos adecuados para la gestión del riesgo en TI.
	RG2.5 Proporcionar aseguramiento independiente sobre la gestión del riesgo en TI.

Proceso	Actividad
RG3	RG3.1 Conseguir que la dirección acepte el enfoque del análisis de riesgo en TI.
	RG3.2 Aprobar el análisis del riesgo en TI.
	RG3.3 Introducir las consideraciones de riesgo en TI en la toma de decisiones de la estrategia del negocio.
	RG3.4 Aceptar el riesgo en TI.
	RG3.5 Priorizar las actividades de respuesta al riesgo en TI.
RE1	RE1.1 Establecer y mantener un modelo para la recolección de datos.
	RE1.2 Recolectar datos sobre los entornos operativos.
	RE1.3 Recolectar datos sobre eventos de riesgo.
	RE1.4 Identificar factores de riesgo.
RE2	RE2.1 Definir el alcance del análisis de riesgo en TI.
	RE2.2 Estimar el riesgo en TI.
	RE2.3 Identificar opciones de respuesta al riesgo.
	RE2.4 Realizar revisiones entre iguales de los análisis de riesgo en TI.
RE3	RE3.1 Mapear recursos de TI a los procesos de negocio.
	RE3.2 Determinar la criticidad para el negocio de los recursos de TI.
	RE3.3 Entender las Capacidades de TI.
	RE3.4 Actualizar los componentes del escenario de Riesgo en TI.
	RE3.5 Mantener el registro y mapa de riesgo TI.
	RE3.6 Desarrollar los indicadores de riesgo TI.
RR1	RR1.1 Comunicar los resultados del análisis de riesgos en TI.
	RR1.2 Informar de las actividades en la gestión del riesgo TI y su estado de cumplimiento.
	RR1.3 Interpretar los hallazgos en la evaluación independiente de TI.
	RR 1.4 Identificar oportunidades asociadas a TI.
RR2	RR2.1 Inventariar los controles.
	RR2.2 Supervisar el alineamiento operativo con los umbrales de tolerancia al riesgo.
	RR2.3 Responder a la exposición y oportunidades de riesgo descubiertos.
	RR2.4 Implementar controles.
	RR2.5 Informar del progreso del plan de acción del riesgo TI.
RR3	RR3.1 Mantener planes de respuesta a incidentes.
	RR3.2 Supervisar el riesgo en TI.
	RR3.3 Iniciar respuesta a incidentes.
	RR3.4 Comunicar lecciones aprendidas de los eventos de riesgo (ISACA, 2009b).

Nota: Información tomada de Marco de Riesgos de TI, ISACA (2009b). Elaborado por los autores: Figueroa F, Hinojosa L.

Guía profesional general de los riesgos de TI

Sección	Subsección	Procesos de dominio del Marco de Referencia de Riesgos								
		RG1	**RG2**	**RG3**	**RE1**	**RE2**	**RE3**	**RR1**	**RR2**	**RR3**
1. Definición de un universo de riesgos y ámbito de gestión de riesgo.		X	X	X		X	X		X	
2. Apetito de riesgo y tolerancia al riesgo		X								
3.Conciencia del riesgo, Comunicación y presentación de informes	Conciencia del riesgo, Comunicación	X	X	X	X	X	X	X	X	X
	Principales indicadores del riesgo y presentación de informes						X	X	X	
	Perfil del riesgo						X			
	Agregación de riesgos	X	X	X				X		
	Cultura de riesgos	X	X							

Sección	Subsección	Procesos de dominio del Marco de Referencia de Riesgos								
		RG1	RG2	RG3	RE1	RE2	RE3	RR1	RR2	RR3
4. Expresando y describiendo el riesgo	Introducción	X	X			X		X		
	Expresando su impacto en términos de negocios	X	X			X		X		
	Describiendo Riesgo-Expresando Frecuencia	X	X			X		X		
	Describiendo Riesgo-Expresando Impacto	X	X			X		X		
	Mapeando los objetivos de negocios de COBIT con otros criterios de impacto	X	X							
	Mapa de Riesgos	X					X	X		
	Registro de Riesgos						X			
5. Escenarios de riesgo	Explicación de los escenarios de riesgo	X				X	X			
	Ejemplo de escenarios de riesgo					X				
	Capacidad de Factores de Riesgo en el Proceso de Análisis de Riesgo	X			X	X	X			
	Factores de Riesgo Ambiental en el Proceso de Análisis de Riesgo	X			X	X				
6. Riesgo de respuesta y asignación de prioridades				X					X	X
7.Un flujo de trabajo de Análisis de Riesgo					X	X	X	X		
8. Mitigación de Riesgos de TI Uso de COBIT y VAL IT (ISACA, 2009b)						X		X	X	X

Nota: Información tomada de Marco de Riesgos de TI, ISACA (2009b). Elaborado por los autores: Figueroa F, Hinojosa L.

Controles asociados entre RISK IT Y COBIT 5

Una vez que se han identificado los controles que forman Risk IT pueden ser asociadas con los dominios y controles de COBIT 5; por ejemplo, se puede asociar el control “RG1.1 Realizar la evaluación del riesgo en TI de la compañía”, está relacionado con la práctica de gobierno de COBIT 5 “EDM03.01 Evaluar la gestión de riesgos” de la siguiente manera:

Tabla 4:

Asociación de RG1.1 de Risk IT vs EDM03.01 de COBIT 5

RISK IT	COBIT 5
RG1.1 Se deben patrocinar talleres con la dirección empresarial para discutir la ampliación de los riesgos. La empresa debe estar dispuesta a aceptar la realización de sus objetivos (apetito por el riesgo). Los administradores de TI ayudan a las empresas a comprender el riesgo en el contexto de situaciones que afectan a su negocio y los objetivos. Es necesario dar de arriba abajo un vistazo a los servicios empresariales y procesos e identificar los principales puntos de soporte de TI. Identificar dónde se genera el valor y donde debe ser protegido y sostenido. Identificar eventos relacionados con la TI y las condiciones que pueden poner en peligro el valor que afectan el rendimiento empresarial y la ejecución de las actividades críticas de negocio dentro de unos límites aceptables Romper los riesgos de TI por líneas de negocio, producto, servicio y proceso. Entender cómo las capacidades de TI contribuyen a la capacidad de la empresa para añadir valor y soportar la pérdida. Identificar donde se concentran las zonas de riesgo, los escenarios, las dependencias, los factores de riesgo y medidas de riesgo que requieren atención de la administración y posteriormente analizar y desarrollar (ISACA, 2009b).	**EDM03.01** Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado (ISACA, 2012a). **APO12.02 Analizar el riesgo.** Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo (ISACA, 2012a). **Actividad 3.** Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual (ISACA, 2012a).

Nota: Elaborado por los autores: Figueroa F, Hinojosa L.

Es decir, el proceso EDM03.01 perteneciente al dominio de COBIT 5 "EDM" puede ser asociado con el control RG1.1 de RISK IT, ya que ambos tratan sobre la evaluación de riesgos de TI. Con esta explicación se puede entender la matriz de asociación de controles que se presenta a continuación:

Tabla 5:

Asociación de RISK IT y COBIT

Prácticas de Gestión Risk IT Cubiertas en COBIT5	EDM01	EDM03	EDM04	APO07	APO12
RG1.1 Realizar la evaluación del riesgo en TI de la compañía.		.01			.02-03

Prácticas de Gestión Risk IT Cubiertas en COBIT5	EDM01	EDM03	EDM04	APO07	APO12
RG1.2 Proponer umbrales de tolerancia del riesgo en TI.		.01			
RG1.3 Aprobar la tolerancia del riesgo en TI.		.01-02			
RG1.4 Alinear la política de riesgo en TI.		.01-02			
RG1.5 Promover una cultura de reconocimiento del riesgo en TI.		.02			
RG1.6 Alentar una comunicación efectiva del riesgo en TI.		.03			
RG2.1 Establecer y mantener la responsabilidad para la gestión del riesgo en TI.		.02			
RG2.2 Coordinar la estrategia del riesgo en TI y del negocio.		.01-02			
RG2.3 Adaptar las prácticas del riesgo en TI a las prácticas del riesgo en la empresa.		.01-02			
RG2.4 Proporcionar los recursos adecuados para la gestión del riesgo en TI.			.01	.01 / .03	
RG2.5 Proporcionar aseguramiento independiente sobre la gestión del riesgo en TI.		.03			
RG3.1 Conseguir que la dirección acepte el enfoque del análisis de riesgo en TI.	.01-02	.02			
RG3.2 Aprobar el análisis del riesgo en TI.		.01			
RG3.3 Introducir las consideraciones de riesgo en TI en la toma de decisiones de la estrategia del negocio.		.01			
RG3.4 Aceptar el riesgo en TI.		.01			
RG3.5 Priorizar las actividades de respuesta al riesgo en TI.		.02			
RE1.1 Establecer y mantener un modelo para la recolección de datos.					.01
RE1.2 Recolectar datos sobre los entornos operativos.					.01
RE1.3 Recolectar datos sobre eventos de riesgo.					.01
RE1.4 Identificar factores de riesgo.					.01
RE2.1 Definir el alcance del análisis de riesgo en TI.					.02
RE2.2 Estimar el riesgo en TI.					.02
RE2.3 Identificar opciones de respuesta al riesgo.					.02
RE2.4 Realizar revisiones entre iguales de los análisis de riesgo en TI.					.02
RE3.1 Mapear recursos de TI a los procesos de negocio.					.02
RE3.2 Determinar la criticidad para el negocio de los recursos de TI.					.03
RE3.3 Entender las Capacidades de TI.					.03
RE3.4 Actualizar los componentes del escenario de Riesgo en TI.					.03
RE3.5 Mantener el registro y mapa de riesgo TI.					.03
RE3.6 Desarrollar los indicadores de riesgo TI.					.03
RR1.1 Comunicar los resultados del análisis de riesgos en TI.					.04

Prácticas de Gestión Risk IT Cubiertas en COBIT5	EDM01	EDM03	EDM04	APO07	APO12
RR1.2 Informar de las actividades en la gestión del riesgo TI y su estado de cumplimiento.					.04
RR1.3 Interpretar los hallazgos en la evaluación independiente de TI.					.04
RR 1.4 Identificar oportunidades asociadas a TI.					.04
RR2.1 Inventariar los controles.					.05
RR2.2 Supervisar el alineamiento operativo con los umbrales de tolerancia al riesgo.					.05
RR2.3 Responder a la exposición y oportunidades de riesgo descubiertos.					.05
RR2.4 Implementar controles.					.05
RR2.5 Informar del progreso del plan de acción del riesgo TI.					.05
RR3.1 Mantener planes de respuesta a incidentes.					.06
RR3.2 Supervisar el riesgo en TI.					.06
RR3.3 Iniciar respuesta a incidentes.					.06
RR3.4 Comunicar lecciones aprendidas de los eventos de riesgo (ISACA, 2009b).					.06

Nota: Las prácticas de gestión de Risk IT fueron tomadas de ISACA (2009b). Elaborado por los autores: Figueroa F, Hinojosa L.

Después de analizar y comparar COBIT 5 y Risk IT es posible señalar que se complementan, ya que RISK IT define prácticas para las organizaciones con el fin de identificar, gobernar y administrar los riesgos asociados al negocio, mismos que son controlados y evaluados a través de las actividades que son establecidas por COBIT para la gestión y control de riesgos, lo que permite que el control y la administración de riesgos en las organizaciones se realice de una forma completa y eficaz dentro del ámbito de las Tecnologías de la Información.

2.1.3 COSO

Instituto de Auditores Internos (2013) señaló que en 1992 el Comité de Organizaciones Patrocinadoras de la Comisión de Normas o Committee of Sponsoring Organizations of the Treadway Commission (COSO) publicó el marco de trabajo Integrado de Control Interno, mismo que ha tenido una gran aceptación y es ampliamente usado a nivel mundial. Es reconocido como líder en su área por diseñar, implementar, conducir y evaluar la efectividad del control interno.

El Instituto de Auditores Internos de España señaló en el 2013 que 20 años después de la inserción de este marco de referencia los ambientes de trabajo y los negocios han cambiado de forma radical, aumentando su complejidad, mejorando su tecnología y avanzando en un mundo globalizado, por lo que el Control Interno es un proceso que se realiza con el propósito de proporcionar una garantía razonable sobre el logro de objetivos de:

- Operaciones: Van de la mano con la misión y visión de la institución.
- Reportes: Se refieren a reportes financieros y no financieros tanto externos como internos.
- Cumplimiento: Se encuentran relacionados con el cumplimiento de Normas y Leyes.

Componentes

El Comité de Organizaciones Patrocinadoras de la Comisión de Normas (COSO) en 2013, (The Committee of Sponsoring Organizations of the Treadway Commission, 2013) numeró 5 componentes, mismos que a su vez fueron desagregados por el Instituto de Auditores Internos de España en el mismo año:

1. Ambiente de control. - Es el conjunto de normas, procesos y estructuras que proveen las bases para llevar a cabo el Control Interno (Instituto de Auditores Internos, 2013). Está formado por 5 principios:

    - Demuestra compromiso con la integridad y los valores éticos.
    - El directorio demuestra independencia de la gerencia y vigila el desarrollo y funcionamiento del Control Interno.
    - La Gerencia establece la estructura, autoridad y responsabilidad.
    - La organización demuestra compromiso con la competencia.
    - Aplica la rendición de cuentas (COSO, 2013).

2. Evaluación del Riesgo. - Involucra un proceso dinámico e interactivo para identificar y analizar riesgos que afectan el logro de objetivos de la entidad, está formada por 4 principios:

    - Especifica objetivos adecuados
    - Identifica y analiza los riesgos
    - Evalúa el riesgo de fraude

- Identifica y analiza cambios significativos (COSO, 2013).

3. Actividades de control. - Son las acciones establecidas por políticas y procedimientos para ayudar a asegurar que las directivas de la administración para mitigar riesgos con el fin de conseguir los objetivos se realicen; comprenden 3 principios:

- Selecciona y desarrolla actividades de control
- Selecciona y desarrolla controles generales sobre la tecnología
- Se implementa a través de políticas y procedimientos (Instituto de Auditores Internos [IAI], 2013).

4. Información y Comunicación. - La Información es necesaria en la entidad para ejercer las responsabilidades de Control Interno con el fin de alcanzar los objetivos; la Comunicación ocurre tanto interna como externamente y provee a la organización de la información necesaria para la realización de controles de forma diaria (IAI, 2013).; se encuentra formada por 3 controles:

- Utiliza la información relevante
- Se comunica internamente
- Se comunica externamente (COSO, 2013).

5. Monitoreo. - Se usan evaluaciones concurrentes, separadas, o una combinación de ambas para determinar si cada uno de los componentes del Control Interno, incluidos los controles para efectivizar los principios de cada componente, se encuentra funcionando (Instituto de Auditores Internos, 2013); cuenta con 2 principios:

- Lleva a cabo evaluaciones en curso y/o separadas
- Evalúa y comunica las deficiencias (COSO, 2013).

Existe una relación directa entre los objetivos, que son los que la entidad se esfuerza en conseguir, los componentes que representan lo que se necesita para lograr los objetivos y la estructura organizacional de la entidad (las unidades operativas, entidades legales, etc.).

Esta relación puede ser representada en un cubo en tres dimensiones:

- Las tres categorías de los objetivos: operaciones, reportes y cumplimiento
- Los 5 componentes representados en cinco filas
- La estructura organizacional de la entidad

Figura 6. Relación Objetivos y Componentes
Fuente: (Gmacagno, 2013)

ISACA (2014) mencionó que dentro de los dominios de COBIT existe el Monitoreo, Evaluación y Cumplimiento (MEA por sus siglas en inglés), el cual contiene un proceso enfocado en cumplimiento, MEA03, que consisten en monitorear, evaluar y cumplir con los requerimientos externos; lo que permite entender que los objetivos de ambos marcos de referencia se relacionan de la siguiente manera:

- Operaciones: Tanto COBIT como COSO son aceptados mundialmente como mejores prácticas de gobierno y administración de procesos relacionados con TI y para el control interno de las compañías de cualquier tipo.
- Reportes: COSO es soportado por los procesos de dominios MEA y los objetivos en cascada de COBIT, con lo que reporta las categorías de una forma objetiva.
- Cumplimiento: Los procesos externos MEA03 están alineados con algunos estándares y marcos de trabajo relevantes como COSO ya que se enfocan en el cumplimiento externo de COBIT.

Tanto COSO como COBIT son usados como la base para auditorías internas, externas y guías de regulación en ciertas industrias ISACA (2014).

Controles asociados entre COSO vs COBIT

Después de identificar y analizar los componentes de COSO pueden ser asociados con los dominios y controles de COBIT 5; por ejemplo, se puede asociar el control "RG1.1 Realizar la evaluación del riesgo en TI de la compañía", está relacionado con la práctica de gobierno de COBIT 5 "EDM03.01 Evaluar la gestión de riesgos" de la siguiente manera:

Tabla 6:

Asociación de RG1.1 de COSO vs EDM03.01 de COBIT 5

COSO	COBIT 5
Ambiente de Control La organización demuestra un compromiso con la integridad y los valores éticos (ISACA, 2014).	**EDM01** Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa (ISACA, 2012a).
	APO01 Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores (ISACA, 2012a).
	APO07 Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada (ISACA, 2012a).

Nota: Elaborado por los autores: Figueroa F, Hinojosa L.

Es decir, los procesos EDM01, APO01 y APO07 pertenecientes a los dominios de COBIT 5 "EDM y APO" puede ser asociado con el primer principio del componente de COSO "Ambiente de control", ya que ambos marcos tratan sobre el nivel de compromiso de la organización y los valores que deben mantener para realizar una buena gestión tanto empresarial como de TI. Con esta explicación se puede entender la matriz de asociación de controles que se presenta a continuación:

Tabla 7:

Asociación de COSO y COBIT

Asociación entre Componentes COSO y controles de COBIT 5							
Nivel empresarial	**Nivel de actividad**	**Área de COBIT**	**Componente COSO**				
			Ambiente de Control	**Evaluación de Riesgos**	**Actividades de Control**	**Información y comunicación**	**Monitoreo**
Evaluar, Orientar y Supervisar							
x		Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno					x
x		Asegurar la Entrega de Beneficios					x
Alinear, Planificar y Organizar							
x		Gestionar el Marco de Gestión de TI	x			x	x
x		Gestionar la Estrategia	x	x		x	x
x		Gestionar la Arquitectura Empresarial			x	x	
x		Gestionar los Recursos Humanos	x			x	
x		Gestionar las Relaciones	x			x	
	x	Gestionar los Acuerdos de Servicio	x		x		x
	x	Gestionar los Proveedores	x	x	x		x
x		Gestionar la Calidad	x		x	x	x
x		Gestionar el Riesgo		x			
Construcción, Adquisición e Implementación							
	x	Gestionar la Identificación y la Construcción de Soluciones			x		
x		Gestionar la Disponibilidad y la Capacidad			x		x
	x	Gestionar los Cambios			x		x
	x	Gestionar la Configuración			x	x	
Entregar, dar Servicio y Soporte							
x		Gestionar las Operaciones		x	x	x	
	x	Gestionar las Peticiones y los Incidentes del Servicio			x	x	x
	x	Gestionar la Continuidad			x	x	
	x	Gestionar los Servicios de Seguridad		x	x	x	x
Supervisión, Evaluación y Verificación							
x		Supervisar, Evaluar y Valorar Rendimiento y Conformidad				x	x
x		Supervisar, Evaluar y Valorar el Sistema de Control Interno					x
x		Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos (ISACA, 2012a)	x				x

Nota: Los componentes de COSO fueron tomados de ISACA (2014). y los dominio de ISACA (2012a). Elaborado por los autores: Figueroa F, Hinojosa L.

COBIT 5 y COSO son dos marcos de referencia complementarios, usados con el objetivo de que las entidades mejoren su proceso de control interno mediante la gestión adecuada de los riesgos empresariales, incluyendo los recursos y activos de TI, estableciendo prácticas de gobierno y gestión que se encuentren alineadas con los objetivos del negocio, esto permite que el control interno sea más eficiente y completo, ya que no abarca únicamente las operaciones financieras de la entidad sino las operaciones e inversiones realizadas en las áreas tecnológicas que apalancan el negocio.

2.1.4 ITIL

Ríos (2011), en su manual ITIL v3 indicó que la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL), es un marco de trabajo que describe un conjunto de mejores prácticas para la entrega de los servicios de Tecnología Informática con alta calidad y eficiencia, 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), que ideó y desarrollo una guía para que las oficinas del sector público británico fueran más eficientes en su trabajo y por tanto se redujeran los costos derivados de los recursos de TI.

El 1 de abril del 2001 la CCTA pasó a formar parte de la OG, que se convirtió así en la nueva propietaria de ITIL, la frase “mejores prácticas” se refiere a un conjunto coherente de acciones que tuvieron éxito en un determinado contexto y que se espera rindan resultados equivalentes en contextos similares.

ITIL en el año 2007 agrupó los elementos principales de ITIL en 5 volúmenes y se desplegó con el nombre de ITIL Versión 3, con un eje de la definición de la estrategia y la mejora continua en el servicio, Office of Government Commerce (2009) señaló que ITIL está definido en 5 fases del ciclo de vida del servicio:

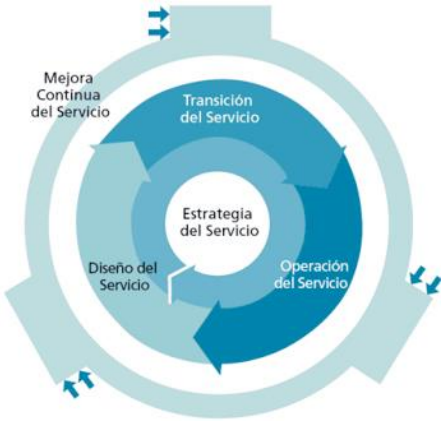

Figura 7 Fases del ciclo de vida del servicio
Fuente: OGC ITIL v3, ciclo de vida del servicio

1. *Estrategia de Servicios - Service Strategy (**SS**).* - Proporciona la guía para diseñar una estrategia en la organización en cuanto a las tecnologías de la información, no sólo como una capacidad organizativa, sino también como un activo estratégico (Ríos, 2011).

2. *Diseño de servicios - Service Design (**SD**).* - Proporciona la guía que permite transformar los objetivos estratégicos en portafolios y activos del servicio, mediante el desarrollo de diseños de arquitecturas, procesos, políticas y documentación; considerando además en la gestión de niveles de servicio, el diseño para gestión de capacidad, continuidad en los servicios TI, gestión de proveedores, y responsabilidades clave en diseño de servicios (Ríos, 2011).

3. *Transición de Servicios - Service Transition (**ST**)* . - Proporciona una guía sobre la gestión de la complejidad relacionada con los cambios en los servicios comunes (del trabajo diario) y en los procesos de gestión del servicio, para evitar consecuencias indeseadas mientras se innova, mejora de capacidades que permitan transformar servicios nuevos y modificados en operaciones, mediante la gestión de la configuración y servicio de activos, planificación de la transición y de apoyo, gestión y despliegue de los Servicios TI, Gestión del Cambio, Gestión del Conocimiento, y por último las responsabilidades y las funciones de las personas que participen en el Cambio o Transición de Servicios (Ríos, 2011).

4. *Operaciones de Servicios - Service Operation(SO).* - Proporciona prácticas para

conseguir y ofrecer un nivel de servicio de la Organización acorde a los requisitos y necesidades de los Clientes (establecimiento del SLA – Service Level Agreement o Acuerdo de Nivel de Servicio), sobre la gestión de Operación del Servicio. Incluye una guía para lograr eficacia y eficiencia en la entrega y en el soporte de servicios que garanticen el valor para el cliente y el proveedor de servicio (Ríos, 2011).

5. *Mejora Continua de Servicios - Continual Service Improvement - (CSI).* - Proporciona una guía instrumental sobre la creación y mantenimiento del valor que se ofrece a los clientes a través de la mejora continua del diseño, introducción y operación de los servicios (Ríos, 2011). Combina principios, prácticas y métodos a partir de la gestión de la calidad, Gestión de Cambios y mejora de la capacidad. De acuerdo con este concepto, las entidades deben estar en constante análisis de sus procesos de negocio, de manera que sean capaces de responder a los objetivos, la estrategia, la competitividad y la gestión de la estructura y organización de las entidades que dispongan de infraestructura de TI (Ríos, 2011).

Las actividades para cada uno de las fases del marco de trabajo ITIL están conformadas de acuerdo al siguiente detalle:

Tabla 8:

Actividades de las fases de ITIL

FASE	SUBPROCESO	ACTIVIDAD
Estrategia del Servicio	**Gestión Financiera (SS1)**	Valoración de Servicio
		Modelo de Demanda
		Optimización del Portafolio de Servicios
		Planeación y Presupuesto
		Analiza las inversiones en Servicios
		Contabilidad y Cargos
		Complimiento de Estándares
		Analiza variables de costo dinámicos (VCD)
	Gestión Estrategia (SS2)	Estrategia de TI
		Estrategia del Negocio
		Evaluar
		Generar
		Ejecutar

FASE	SUBPROCESO	ACTIVIDAD
	Gestión Demanda (SS3)	Análisis y codificación de Patrones de Actividad del Negocio (PBA)
		Perfiles de Usuario
		Desarrollo de Paquetes de Servicio (SDP)
		Definición de Paquetes de Niveles de Servicio
	Gestión Cartera de Servicios (SS4)	Define
		Analiza
		Aprueba
		Comunica
		Bajo Desarrollo
		Catálogo
		Retirados
Diseño del Servicio	**Gestión del Catálogo de Servicios (SD1)**	Definición de los Servicios
		Producir y Mantener el Catálogo de Servicios
		Vistas del Catálogo
		Interfaz con la Gestión del Porfolio
	Gestión de Niveles de Servicios (SD2)	Determinar Requerimientos
		Realizar los SLAs (Service Level Agreement)
		Monitorear y Reportar
		Mejorar Satisfacción del Cliente
		Conducir revisión del Servicio
		Revisar SLAs y Contratos
		Desarrollo de Relaciones
	Gestión de la capacidad (SD3)	Revisar la Capacidad Actual
		Producir el Plan de Capacidad
		Mejorar la Capacidad
		Revisar, Acordar y Documentar requerimientos
		Sub-procesos (Negocio, Servicio y Componente)
	Gestión de la disponibilidad (SD4)	Monitorear, Medir, Analizar, Reportar y Revisar
		Investigar
		Evaluar y Gestionar el Riesgo
		Implementar contra medidas
		Planear y diseñar
		Revisar y Probar
	Gestión de la continuidad de Servicios de TI (SD5)	Inicializar el proyecto
		Determinar requerimientos
		Producir una estrategia
		Desarrollar planes
		Implementar estrategia
		Operación en marcha
		Invocación del Plan
	Gestión de Seguridad de la Información (SD6)	Política de seguridad de la Información (IPT)
		Implementar y Mejorar los Controles de Seguridad.
		Iniciar el Análisis de Impacto al Negocio (BIA)
		Gestionar Brechas de Seguridad
		Desarrollar Revisiones, Auditorias y Pruebas
		Gobierno de Seguridad de la Información (ISO 27000)
	Gestión de Suministradores (SD7)	Evaluar
		Establecer
		Categorizar proveedores
		Mantener la SCD
		Gestionar el desempeño
		Renovar y/o Terminar

FASE	SUBPROCESO	ACTIVIDAD
Transición del Servicio	Planeación de la Transición y Soporte (ST1)	Definir la estrategia de Transición
		Preparar la transición del Servicio
		Planear y coordinar la transición del servicio
		Aconsejar
		Proporcionar Administración
		Monitorear e informar sobre el proceso
	Gestión de Cambios (ST2)	Comité Asesor de Cambios (CAB)
		Crear y registrar el RFC
		Revisar el RFC
		Evaluar los cambios
		Autorizar los cambios
		Planear actualizaciones
		Coordinar la implementación de cambios
		Revisar y cerrar un cambio
	Gestión de la Configuración y de los activos del servicio (ST3)	Gestión y planificación
		Identificación de la configuración
		Control de la configuración
		Seguimiento e información del estado
		Auditoría y verificación
		Base de datos de la configuración
	Gestión de Entrega y Despliegue (ST4)	Plan de Implementación de un Paquete
		Preparación para construcción, prueba e implementación
		Construcción y Pruebas
		Pruebas del Servicio y Pilotos
		Planear y preparar para la implementación
		Desarrollar la transferencia, implementación y Retiro
		Verificar la implementación
		Apoyo en la puesta en Marcha
		Revisar y cerrar la implementación
		Revisar y cerrar la transición del servicio
	Validación y Pruebas del Servicio (ST5)	Administración de la Validación y Pruebas
		Plan y Diseño de Pruebas
		Verificación del plan de pruebas y del diseño de pruebas
		Preparar el entorno de pruebas
		Realizar las pruebas
		Evaluar criterios de salida e informes
		Entornos de pruebas y Cierre
	Evaluación del cambio (ST6)	Plan de Evaluación
		Evaluar el rendimiento Previsto
		Evaluar el rendimiento Actual
	Gestión del conocimiento (ST7)	Definir la estrategia de la Gestión del conocimiento
		Transferir el Conocimiento
		Gestión de Datos e Información
		Usar el Sistema de Gestión del conocimiento del Servicio (SKMS)
Operación del Servicio	Gestión de Eventos (SO1)	Notificación de Eventos
		Detección de Eventos
		Filtro de eventos
		Categorización de eventos
		Correlación de eventos
		Respuesta a disparadores
		Selección de Respuestas
		Revisar acciones
		Cierre de eventos
		Identificar incidentes

FASE	SUBPROCESO	ACTIVIDAD
	Gestión de Incidentes (SO2)	Registrar Incidentes
		Categorizar Incidentes
		Priorizar incidentes
		Ejecutar Diagnósticos
		Escalar Incidentes
		Investigar y diagnosticar
		Incidentes
		Resolver y recuperar incidentes
		Cerrar incidentes
	Gestión de Requerimientos (SO3)	Seleccionar e ingresar detalles de Requerimientos de Servicios
		Aprobar requerimientos de servicio
		Requerimientos de Servicios Cumplidos
		Cerrar Requerimientos de Servicios
	Gestión de Problemas (SO4)	Detectar Problemas
		Registrar Problemas
		Categorizar Problemas
		Priorizar Problemas
		Investigar y diagnosticar Problemas
		Encontrar Soluciones Temporales
		Registrar Errores Conocidos
		Resolver Problemas
		Cerrar Problemas
		Revisar Problemas Principales
	Gestión de Accesos (SO5)	Requerimientos de Acceso
		Verificación de Requerimientos
		Proveer Permisos
		Monitorear, mantener usuarios, Roles y Grupos
		Registro y rastreo de accesos
		Remover o restringir Permisos (Ríos, 2011)
MCS	**Proceso de mejora en 7 pasos (CSI1)**	Integración con el resto de etapas del ciclo de vida y procesos de gestión del servicio
		Métricas y medidas
	Informes del servicio (CSI2)	Políticas y normas de los informes

Nota: Fases y subprocesos tomado de Ríos (2011). Elaborado por los autores: Figueroa F, Hinojosa L.

Mapa de Procesos y funciones ITIL V3

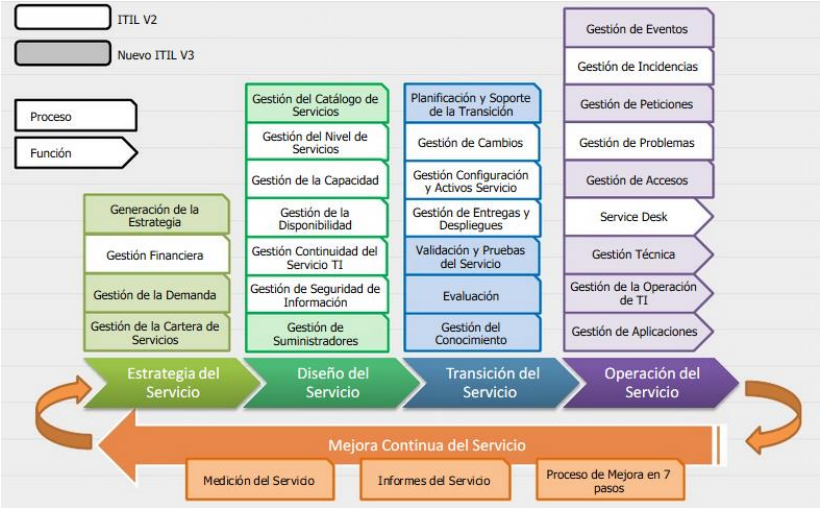

Figura 8 Mapa de procesos ITIL
Fuente: www.OverTI.es, 2009

COBIT 5 e ITIL V3 están alineados y no presentan contradicciones. Pero no son idénticos puesto que están desarrollados desde perspectivas diferentes: COBIT 5 desde el negocio a las TI, e ITIL desde las TI al negocio.

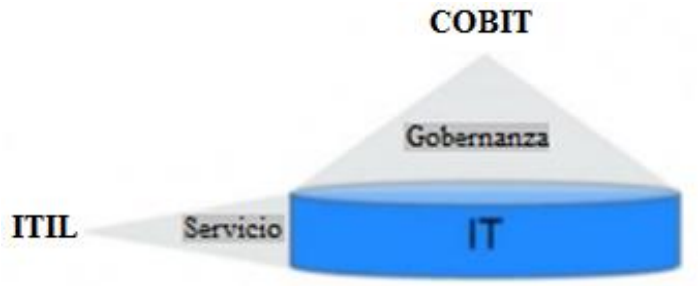

Figura 9 Perspectiva COBIT vs ITIL
Fuente: elaborada por los autores: Figueroa F, Hinojosa L.

Controles asociados entre ITIL Y COBIT 5

Después de identificar y analizar las fases de ITIL pueden ser asociadas con los dominios y controles de COBIT 5; por ejemplo, se puede asociar la fase "Gestión del servicio", está relacionado con la práctica de gobierno de COBIT 5 "APO02 Gestionar la Estrategia" de la siguiente manera:

Tabla 9:

Asociación de la fase de Gestión del servicio de ITIL vs APO02 de COBIT 5

ITIL	COBIT 5
Gestión del servicio El objetivo principal de la etapa de Diseño del Servicio del ciclo de vida es el diseño de servicios nuevos o modificados para su introducción en el entorno de producción. Es importante que se adopte un método integral para todos los aspectos del diseño, y que al modificar o cambiar cualquier elemento individual del diseño, se consideren todos los demás aspectos (Ríos, 2011).	**APO02. Gestionar la Estrategia** Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos (ISACA, 2012a).

Nota: Elaborado por los autores: Figueroa F, Hinojosa L.

Es decir, el proceso APO02 perteneciente al dominio de COBIT 5 "APO" puede ser asociado con la fase de "Gestión del servicio" de ITIL, ya que ambos marcos buscan la correcta gestión de servicios tanto internos como externos para una correcta administración de los activos y recursos de TI. Con esta explicación se puede entender la matriz de asociación de controles que se presenta a continuación:

Tabla 10:

Asociación de Controles ITIL y COBIT 5

	ITIL		COBIT 5			
	Fase	**Libro**	**APO**	**BAI**	**DSS**	**MEA**
Estrategia del Servicio	Gestión del servicio	SS 2.1 SS 2.3 SS 2.4	02			
	Servicios y creación de valor	SS 2.2	09			
	Activos del servicio	SS 3.2 SS B.1		10		
	Estructuras de servicios	SS 3.4	09			
	Fundamentos de estrategias	SS 3.5	02			
	Abastecimiento	SS 6.5	10			

	ITIL		COBIT 5			
	Fase	**Libro**	**APO**	**BAI**	**DSS**	**MEA**
	Tecnología y estrategia	SS 8	02			
	Automatización del servicio	SS 8.1	09			
	Gestión de riesgos	SS 9.5	12			
	Creación de la estrategia de servicio	SS 4	02			
	Preparación para la ejecución	SS 7	02			
	Gestión financiera de TI	SS 5.1 SO 4.6.7	02, 06			
	Valoración del servicio y análisis de impacto en el negocio	SS 5.1.1 SS 5.1.3.4	06			
	Modelos de suministro de servicios, análisis y optimización	SS 5.1.2.4 SS 5.1.3.2	06			
	Importancia del portafolio de servicios	SS 5.3	09			
Diseño del Servicio	Principios del diseño	SD 3	01			
	Objetivos	SD 2.4.1 SD 3.1	09			
	Alcances	SD 2.4.2	09			
	Actividades y consideraciones de las tecnologías relacionadas al diseño de servicios	SD 5 SD 5.1 SD 5.2	09			
	Implementar el diseño del servicio	SD 8.2 SD 8.3 SD 8.4	09			
	Apéndices del diseño de servicios	Apéndice A	09			
		Apéndice B	09	02		
		Apéndice E			01, 05	
		Apéndice G	09			
		Apéndice H				01
	Gestión de niveles de servicios	SD 4.2	09			
	Gestión de capacidad	SD 4.3, ST, SO		04		
	Propósito, valor y conceptos	SD 4.3		04		
	Gestión de proveedores	SD 4.7	10			
Transición del servicio	Actividades operacionales comunes	ST 5.1 ST 5.2 ST 5.3		06		
	Organización para la transición de servicios	ST 6.0	01			

	ITIL		COBIT 5			
	Fase	**Libro**	**APO**	**BAI**	**DSS**	**MEA**
	Gestión de cambios	ST 4.2		06		
	Consejo consultivo de cambios	ST 4.2.6.8		06		
	Gestión de la configuración y de los activos del servicio	SS, SD, ST 4.3, SO		10		
	Propósito, objetivos y valor	ST 4.3.1 ST 4.3.2 ST 4.3.3		10		
	Políticas	ST 4.3.4.1		10		
	Conceptos básicos	ST 4.3.4.2		10		
	Sistema de Gestión de la Configuración	ST 4.3.4.3		10		
	Gestión de la liberación e implementación	SD, ST 4.4, SO		07		
	Validación y prueba del servicio	ST 4.5		07		
Operación del Servicio	Fundamentos	SO 2.4			01	
	Principios	SO 3.4	09			
	Organización para la operación del servicio	SO 6.4			01	
		SO 6.5		02		
	Gestión de eventos	SO 4.1		04	01, 02	
	Atención de peticiones	SO 4.3		06		
	Políticas, principios y modelos de requerimientos	SO 4.3.4		06		
	Gestión de incidentes	ST, SO 4.2			02	
	Propósito, alcance, valor, políticas, principios y conceptos	SO 4.2.4			02	
	Gestión de la información	SO 4.2.7			02	
	Métricas de la gestión de incidentes	SO 4.2.8			02	
	Gestión de problemas	ST, SO 4.4			03	
	Gestión de aplicaciones	SO 6.5		02		
	Gestión de operaciones	SO 5 SO 6.4			01	
	Estructura de la gestión de operaciones de TI	SO 6.4			01	
	Monitoreo y control	SO 5.1		04	01	
	Actividades operacionales de procesos cubiertos en otras fases del ciclo de vida	SO 4.6.2		10		

	ITIL		COBIT 5			
	Fase	**Libro**	**APO**	**BAI**	**DSS**	**MEA**
		SO 4.6.3		07		
		SO 4.6.4		04		
		SO 4.6.7	06			
		SO 4.6.8			04	
Mejoramiento continuo de los Servicios	Principios y enfoque de CSI	CSI 2.4 CSI 3.1 CSI 3.2 CSI 3.3 CSI 3.4 CSI 4.3.12				01
	Mejora de los servicios	CSI 3.5 CSI 3.6 CSI 3.7 CSI 3.8 CSI 3.9	09			
	Gestión de niveles de servicio	CSI 4.6	09			
	Mejora continua en los procesos del ciclo de vida de la Gestión de los Servicios (Ríos, 2011)	CSI 5.6		06, 07, 08	03	

Nota: Fases tomadas de Ríos (2011). Elaborado por los autores: Figueroa F. Hinojosa L.

ITIL Y COBIT se complementan, de forma que ITIL describe cómo realizar las actividades desde el punto de vista de los servicios de TI mapeados a los procesos de negocio para lograr efectividad y eficiencia en los servicios de TI y a su vez COBIT describe qué actividades realizar desde el punto de vista del gobierno corporativo para verificar la conformidad en cuanto a disponibilidad, rendimiento, eficiencia y riesgos asociados a los servicios de TI.

2.1.5 ISSAI (International Standards of Supreme Audit Institutions)

Las Normas Internacionales de Auditoría de las Entidades Fiscalizadoras Superiores fueron creadas por la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), y buscan promover una auditoría independiente y eficaz dentro de las Entidades Fiscalizadoras Superiores (EFS) mediante la credibilidad, calidad y profesionalismo de la fiscalización en el sector público (INTOSAI, 2015).

El Marco de Normas Profesionales de la INTOSAI tiene 4 niveles:

- Nivel 1. - Contiene los principios fundamentales del marco.
- Nivel 2. - Establece requisitos previos para el funcionamiento apropiado de las Entidades Fiscalizadoras Superiores (EFS).
- Nivel 3 y 4. - Conducción de auditorías individuales que respaldan la fiscalización eficaz e independiente de las entidades del sector público.

En las ISSAIs emitidas por la INTOSAI existe una "*Metodología para la Revisión de la Seguridad de los Sistemas de Información*", la cual sirve como guía para ayudar a las EFS que deben revisar la seguridad de los sistemas de información, pueden ser usados para comprender los sistemas y comparar el costo con la efectividad de los mismos; no establece un detalle de pasos a seguir para la auditoría sino es una descripción estructurada para ayudar y administrar los riesgos en los sistemas de información (INTOSAI, 2013).

INTOSAI (2013) señaló que la metodología establece un enfoque en dos niveles para la revisión de la seguridad de los sistemas de información, con el objetivo de balancear el costo de la seguridad pensando en el tipo de información que se va a salvaguardar. Esto provee opciones al escoger la metodología entre una muy sofisticada y una muy formal y recursiva.

Así también, la INTOSAI en el año 2013 implantó un método vertical de revisión de la seguridad de la información y trata de optar por una perspectiva gerencial en caso de que el tipo de información sea valiosa para la organización, validando cuales son los riesgos a los que se encuentra expuesta y las recomendaciones que se pueden realizar; este método recae sobre evaluaciones cualitativas de los riesgos y el impacto que podrían tener si ocurren, la evaluación se la realiza inicialmente de forma individual, y posteriormente de forma global para determinar la exposición al riesgo. Entre las ventajas se encuentran que no son necesarios grandes recursos económicos y que es fácil de usar, se lo ejecuta de forma manual y puede ser aplicado por cualquier EFS con personal que conozca de sistemas de información y controles.

La Organización Internacional de Entidades Fiscalizadoras Superiores en el año 2013, mencionó que para usar estas metodologías se debe planificar la revisión incluyendo al menos los siguientes puntos:

- Conocer la entidad y el entorno
- Definir el alcance de la revisión: sistemas de información con sus límites físicos, lógicos y geográficos.
- Recursos disponibles: consultores calificados, presupuestos y periodos de tiempo.
- Disponibilidad de estadísticas de amenazas y costos.
- Reportes: usuarios, contextos, tipos de reportes y recomendaciones necesarias sobre los mismos.
- Método de revisión: Vertical, análisis detallado o una combinación de ambos.

Finalmente, las ISSAIs proponen métodos detallados de seguridad de los sistemas de información, los cuales son análisis y administración de riesgos, basados en un análisis cuantitativo y cualitativo de los activos/información de los sistemas; con el objetivo de medir el impacto monetario de la exposición de la información a riesgos de seguridad y las contramedidas para mitigar estos riesgos (INTOSAI, 2013).

Para usar ésta metodología detallada es importante considerar:

- Contar con experiencia en tecnologías de la información y seguridad de la información.
- Disponibilidad de una metodología completa
- Disponibilidad de un paquete informático completo que soporte las revisiones: métodos cuantitativos de riesgos para realizar tareas puntuales con el fin de garantizar una revisión minuciosa de los riesgos.
- Presupuesto para adaptar el sistema que se usará al ambiente de revisión.
- Presupuestos en capacitación en caso de no conocer lo que se revisará.
- Recursos financieros y de tiempo.
- La necesidad de realizar una evaluación detallada sobre información que justifique la revisión.

La determinación de lo que se debe revisar en el proceso de evaluación de un sistema de seguridad, involucra:

- Declaración de activos: un listado de activos que se tengan en ámbito de seguridad de la información.
- Evaluación de impacto en el negocio: evaluar qué podría causar un impacto en el negocio al ser vulnerado.
- Evaluación de riesgos y amenazas: determinar los riesgos que podrían ocurrir.
- Exposición de la seguridad existente: evaluar el impacto del negocio y las amenazas en conjunto para determinar la exposición general de la organización.
- Decisiones de seguridad y recomendaciones: tomar decisiones sobre la seguridad para minimizar los riesgos.

Tasa de exposición	Decisión de seguridad	Acción Recomendada
ALTO (9,8,7)	Controlar el riesgo	Implementar políticas adicionales y medidas (estándares, procedimientos y herramientas)
MEDIO (6,5,4)	Controlar el riesgo Evitar el Riesgo	Implementar políticas adicionales y medidas Cambiar / Mejorar los procedimientos operacionales
BAJO (3,2 ,1)	Evitar el Riesgo Limitar el Riesgo Aceptar el Riesgo(INTOSAI, 2013)	Cambiar / Mejorar los procedimientos operacionales Obtener cobertura de seguro No cambiar/Continuar como estaba planeado

Figura 10. Revisión de seguridad ISSAIs
Fuente: Información tomada de Matriz de riesgos(INTOSAI, 2013) *y traducida por los autores: Figueroa F. Hinojosa*

Controles asociados entre ISSAI vs COBIT

Después de identificar y analizar los controles implementados por las ISSAIs pueden ser asociados con los dominios y controles de COBIT 5; por ejemplo, el control de "Administración de la Seguridad", está relacionado con las prácticas de gobierno de COBIT 5 "APO13 y DSS05" de la siguiente manera:

Tabla 11:

Asociación del control Administración de la seguridad de ISSAI vs APO13 y DSS05 de COBIT 5

ISSAI	COBIT 5
Administración de la seguridad Uno de los activos clave de la organización es la información. El primer paso para salvaguardar los bienes tecnológicos es adoptar políticas de gestión de la información y medidas que abarquen principios de gestión de la seguridad. Las medidas de seguridad adoptadas deben: • Ser consistente con el valor de la información. • Mantenerse con la información mientras es procesada o trasladada. • Ser continua en todas las situaciones (INTOSAI, 2013).	**APO13. Gestionar la Seguridad** Definir, operar y supervisar un sistema para la gestión de la seguridad de la información. **DSS05. Gestionar Servicios de Seguridad** Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad (ISACA, 2012a).

Nota: Elaborado por los autores: Figueroa F, Hinojosa L.

Es decir, los procesos APO13 y DSS05 perteneciente a los dominios de COBIT 5 "APO y DSS" pueden ser asociados con el control "Administración de la Seguridad" de las ISSAIs, ya que el objetivo de ambos marcos es gestionar o administrar la seguridad de la información desde un punto de vista gerencial. Con esta explicación se puede entender la matriz de asociación de controles que se presenta a continuación:

Tabla 12:

Alineación ISSAIs y COBIT 5

Medidas de seguridad ISSAI	Dominio de COBIT				
	EDMA	**APO**	**BAI**	**DSS**	**MEA**
Evolución de la Gestión de la Información	04		09	05	02
Administración de la seguridad		13		05	
Equipo de Seguridad	04	07 - 13	08		
Procesos	01 - 13			05	
Evaluación de riesgos y amenazas	03	08 - 12	01		
Evaluación del impacto en el negocio		01 - 03	04	02 - 04 - 06	01
Clasificación de exposición de seguridades (INTOSAI, 2013)		13			02

Nota: Las medidas de seguridad de ISSAI fueron tomadas de INTOSAI (2013). Elaborado por los autores: Figueroa F. Hinojosa L.

Las Normas Internacionales de Auditoría de las Entidades Fiscalizadoras Superiores (ISSAI) y COBIT 5 cuentan con controles en común con la diferencia de que las ISSAIs se refieren exclusivamente a lineamientos sobre seguridad de la información; mientras que COBIT abarca todos los aspectos comprendidos por las TI desde el Gobierno de las Tecnologías de la Información hasta los procesos de almaceamiento de datos.

2.1.6 ISO 27002

En el 2007 la norma ISO 17799:2005 cambió su nombre a ISO 27002, la cual es una guía de buenas prácticas en la que se describen los objetivos de control y los controles para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización, sin importar su naturaleza ni el giro de negocio en el que se apliquen; éstos se encuentran distribuidos de la siguiente manera (Grupa, 2015a).:

- 11 Dominios
- 39 Objetivos de control
- 133 Controles

La norma ha ido evolucionando con el pasar del tiempo, de la versión ISO 27002:2007 pasó a la versión ISO 27002:2013 y en cada una de éstas versiones los controles han sufrido algunas modificaciones distribuidos de la siguiente manera (Disterer, 2013).:

- 14 Dominios
- 35 Objetivos de control
- 114 Controles

Sin embargo, se puede señalar que los dominios continúan formando capítulos, centrándose en un aspecto determinado de la seguridad de la información, con las siguientes cláusulas (Grupa, 2015a).:

Figura 11. ISO 27002
Fuente: Iso27002nor.blogspot.com

- *Política de Seguridad.* - Se define que la Dirección debería establecer una política de seguridad que se encuentre alineada a los objetivos del negocio para proteger la seguridad de la información.
- *Organización de la seguridad de la información.* - Debe existir una asignación de roles de seguridad y organización la implementación de seguridad de la información en toda la organización tanto de manera interna como relacionada con terceros que tienen acceso a la institución.
- *Gestión de activos.* - Identificar los activos físicos, servicios informáticos y de comunicaciones, recursos de información y de software que posee la entidad, de manera que se logre mantener la protección adecuada de los activos de la organización a través de la designación de un responsable de los mismos.
- *Seguridad de los recursos humanos.* - Tomar acciones sobre la contratación de personal mediante la generación de acuerdos, así también los empleados deben mantener una capacitación y concientización continua sobre temas de seguridad de la información; y emitir controles sobre roles y perfiles asignados a los empleados, contratistas o terceras personas.

- *Seguridad física y del entorno.* – Evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la organización. Los servicios de procesamiento de información sensible o crítica deberían estar ubicados en áreas seguras, protegidas por perímetros de la seguridad definidos, con barreras de seguridad y controles de entrada adecuados.
- *Gestión de comunicaciones y operaciones.* - Se deben definir procedimientos y responsabilidades sobre las operaciones de todos los servicios de procesamiento de información (protección contra amenazas como malware, virus, etc.; soporte y planes de recuperación; gestión de redes; controles para intercambio de software e información; cuidar de los servicios electrónicos como pagos en línea, correo electrónico); y se debe verificar el cumplimiento de las normas, procedimientos y controles establecidos mediante auditorías técnicas y registros de actividad de los sistemas (pistas, bitácoras) como base para el monitoreo permanente del estado del riesgo en los sistemas y descubrimiento de nuevos riesgos.
- *Control de acceso.* - Se deben conocer los requerimientos de la entidad para gestionar un adecuado control de usuarios, control acceso físico y lógico a las redes, a los sistemas operativos, a las aplicaciones; y mantener controlados los dispositivos móviles que acceden a la red.
- *Adquisición, desarrollo y mantenimiento de los sistemas de información.* - Considerar los requisitos de seguridad que deben tener los sistemas, así también las aplicaciones, mantener controles criptográficos, validar que existan seguridades para los archivos del sistema, mantener seguridad al desarrollar o dar soporte al software y gestionar las vulnerabilidades técnicas que se presenten.

- *Gestión de incidentes de seguridad de la información.* - Se debe asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se reporten tan pronto como sea posible de forma que permiten tomar acciones correctivas oportunamente.
- *Gestión de continuidad del negocio.* – Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna, mediante un plan que garantice la continuidad del negocio para reducir al mínimo las interrupciones que pueden presentarse.
- *Cumplimiento.* – Se debe evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de la seguridad a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos.

Controles asociados entre ISO/IEC 27002:2013 vs COBIT

Una vez que los controles de la Norma ISO/IEC 27002:2013 han sido identificados y analizados es posible asociarlos con los dominios y controles de COBIT 5; por ejemplo, el control de "6.1.1 Asignación de responsabilidades para la seguridad de la información", está relacionado con las prácticas de gobierno de COBIT 5 "APO01 y APO02" de la siguiente manera:

Tabla 13:

Asociación del control 6.1.1 de ISO/IEC 27002:2013 vs APO01 y APO02 de COBIT 5

ISO/IEC 27002:2013	COBIT 5
4.1.1 Asignación de responsabilidades para la seguridad de la información Se deberían definir y asignar claramente todas las responsabilidades para la seguridad de la información (Grupa, 2015b).	**APO01. Gestionar el Marco de Gestión de TI** Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores (ISACA, 2012a) **.**
	APO02. Gestionar la Estrategia Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos (ISACA, 2012a),

Nota: Elaborado por los autores: Figueroa F, Hinojosa L.

Es decir, los procesos APO01 y APO02 perteneciente al dominio de COBIT 5 "APO" pueden ser asociados con el control "6.1.1. Asignación de responsabilidades para la seguridad de la información" de la Norma ISO 27002:2013, debido a que tanto el Marco de Referencia como la Norma tratan de asignar responsables sobre la información de la organización, de forma que se pueda mitigar el riesgo de la pérdida de las propiedades de la seguridad sobre la información. Con esta explicación se puede entender la matriz de asociación de controles que se presenta a continuación:

Tabla 14:

Alineación de ISO 27002:2013 y COBIT 5

Controles ISO/IEC 27002:2013	Dominio de COBIT				
	EDM	APO	BAI	DSS	MEA
5.1.1 Conjunto de políticas para la seguridad de la información		01		05	02
5.1.2 Revisión de las políticas para la seguridad de la información.		01			
6.1.1 Asignación de responsabilidades para la seguridad de la información		01			
6.1.2 Segregación de tareas		01		05	
6.1.3 Contacto con las autoridades		01-02-04		04	
6.1.4 Contacto con grupos de interés especial		13			
6.1.5 Seguridad de la información en la gestión de proyectos			01	05	
6.2.1 Política de uso de dispositivos para movilidad				05	
6.2.2 Teletrabajo		01-04		05	
7.1.1 Investigación de antecedentes		07			
7.1.2 Términos y condiciones de contratación		07			
7.2.1 Responsabilidades de gestión		01			
7.2.2 Concienciación, educación y capacitación en seguridad de la información		07	03		
7.2.3 Proceso disciplinario		07			
7.3.1 Cese o cambio de puesto de trabajo			09	05	
8.1.1 Inventario de activos			09	01-05	
8.1.2 Propiedad de los activos		01			
8.1.3 Uso aceptable de los activos		01		06	
8.1.4 Devolución de activos.			09		
8.2.1 Directrices de clasificación		07		06	
8.2.2 Etiquetado y manipulado de la información.				06	
8.2.3 Manipulación de activos.				06	
8.3.1 Gestión de soportes extraíbles.				05	
8.3.2 Eliminación de soportes.			09	05	
8.3.3 Soportes físicos en tránsito				05	
9.1.1 Políticas de control de acceso				01-05	
9.1.2 Control de acceso a las redes y servicios asociados.				05	
9.2.1 Gestión de altas/bajas en el registro de usuarios.				05	
9.2.2 Gestión de los derechos de acceso asignados a usuarios.				05	
9.2.3 Gestión de los derechos de acceso con privilegios especiales.				05	
9.2.4 Gestión de información confidencial de autenticación de usuarios.				05	
9.2.5 Revisión de los derechos de acceso de los usuarios.				05	
9.2.6 Retirada o adaptación de los derechos de acceso				05	
9.3.1 Uso de información confidencial para la autenticación		07		05	
9.4.2 Procedimientos seguros de inicio de sesión.				05	
9.4.3 Gestión de contraseñas de usuario.				05	
9.4.4 Uso de herramientas de administración de sistemas.				05	
9.4.5 Control de acceso al código fuente de los programas		13			
10.1.1 Política de uso de los controles criptográficos.				05	

Controles ISO/IEC 27002:2013	Dominio de COBIT				
	EDM	APO	BAI	DSS	MEA
10.1.2 Gestión de claves				05	
11.1.1 Perímetro de seguridad física.				05	
11.1.2 Controles físicos de entrada.				05	
11.1.3 Seguridad de oficinas, despachos y recursos.				05	
11.1.4 Protección contra las amenazas externas y ambientales				01	
11.1.5 El trabajo en áreas seguras				05	
11.1.6 Áreas de acceso público, carga y descarga				05	
11.2.1 Emplazamiento y protección de equipos.				05	
11.2.2 Instalaciones de suministro.				01	
11.2.3 Seguridad del cableado.				01	
11.2.4 Mantenimiento de los equipos.		11			
11.2.5 Salida de activos fuera de las dependencias de la empresa.				05	
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones				03	
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.		11			
11.2.8 Equipo informático de usuario desatendido.				05	
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla				05	
12.1.1 Documentación de procedimientos de operación.				01	
12.1.2 Gestión de cambios.		07			
12.1.3 Gestión de capacidades.		04			
12.1.4 Separación de entornos de desarrollo, prueba y producción				05	
12.2.1 Controles contra el código malicioso.				05	
12.3.1 Copias de seguridad de la información				04	
12.4.1 Registro y gestión de eventos de actividad.				05	
12.4.2 Protección de los registros de información.				05	
12.4.3 Registros de actividad del administrador y operador del sistema.				05	
12.4.4 Sincronización de relojes				01	
12.5.1 Instalación del software en sistemas en producción.				01	
12.6.1 Gestión de las vulnerabilidades técnicas.				03	
12.6.2 Restricciones en la instalación de software				01	
12.7.1 Controles de auditoría de los sistemas de información		03			
13.1.1 Controles de red				05	
13.1.2 Mecanismos de seguridad asociados a servicios en red.				05	
13.1.3 Segregación de redes				05	
13.2.1 Políticas y procedimientos de intercambio de información				05	
13.2.2 Acuerdos de intercambio		07-10			
13.2.3 Mensajería electrónica				05	
13.2.4 Acuerdos de confidencialidad y secreto			03-07		
14.1.1 Análisis y especificación de los requisitos de seguridad.		03			
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.				05	
14.1.3 Protección de las transacciones por redes telemáticas				05	
14.2.1 Política de desarrollo seguro de software.		03			
14.2.2 Procedimientos de control de cambios en los sistemas.		07			

Controles ISO/IEC 27002:2013	Dominio de COBIT				
	EDM	APO	BAI	DSS	MEA
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.		09			
14.2.4 Restricciones a los cambios en los paquetes de software.		01			
14.2.5 Uso de principios de ingeniería en protección de sistemas.		03			
14.2.6 Seguridad en entornos de desarrollo.		03			
14.2.7 Externalización del desarrollo de software.		03			
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas			03		
14.2.9 Pruebas de aceptación			07		
14.3.1 Protección de los datos utilizados en pruebas			03		
15.1.1 Política de seguridad de la información para suministradores		10			
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores		10			
15.1.3 Cadena de suministro en tecnologías de la información y comunicación				04	
15.2.1 Supervisión y revisión de los servicios prestados por terceros.		10			
15.2.2 Gestión de cambios en los servicios prestados por terceros.		07			
16.1.1 Responsabilidades y procedimientos.				03	
16.1.2 Notificación de los eventos de seguridad de la información.				02	
16.1.3 Notificación de puntos débiles de la seguridad.				03	
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.				03	
16.1.5 Respuesta a los incidentes de seguridad.				02	
16.1.6 Aprendizaje de los incidentes de seguridad de la información.				03	
16.1.7 Recopilación de evidencias.				05	
17.1.1 Planificación de la continuidad de la seguridad de la información				04	
17.1.2 Implantación de la continuidad de la seguridad de la información.				04	
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	01				
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información		04			
18.1.1 Identificación de la legislación aplicable		07			
18.1.2 Derechos de propiedad intelectual (DPI).		03			
18.1.3 Protección de los registros de la organización				05	
18.1.4 Protección de datos y privacidad de la información personal					03
18.1.5 Regulación de los controles criptográficos				05	
18.2.1 Revisión independiente de la seguridad de la información.					02
18.2.2 Cumplimiento de las políticas y normas de seguridad					02
18.2.3 Comprobación del cumplimiento.					02

Nota: Los controles de ISO/IEC 27002:2013 fueron tomados de Iso27000.es (2013). Elaborado por los autores: Figueroa F, Hinojosa L.

El estándar ISO 27002 en su versión 2013 y COBIT 5 se complementan para poder formar un plan de seguridad de la información, ambos emiten controles para salvaguardar las propiedades de la información; es decir, que sea íntegra, confiable y se encuentre disponible, la diferencia radica en que COBIT emite controles más gerenciales y generales, mientras ISO propone una cantidad de controles con mayor detalle sobre los activos y recursos de TI en las organizaciones.

2.1.7 COBIT 5

ISACA entregó la nueva edición de este marco de referencia el 10 de abril del 2012, esta actualización proporciona una visión empresarial del Gobierno de TI que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas.

COBIT 5 parte de COBIT 4.1, y a la vez se integra con importantes marcos como Val IT y Risk IT, Information Technology Infrastructure Library y las normas ISO relacionadas.

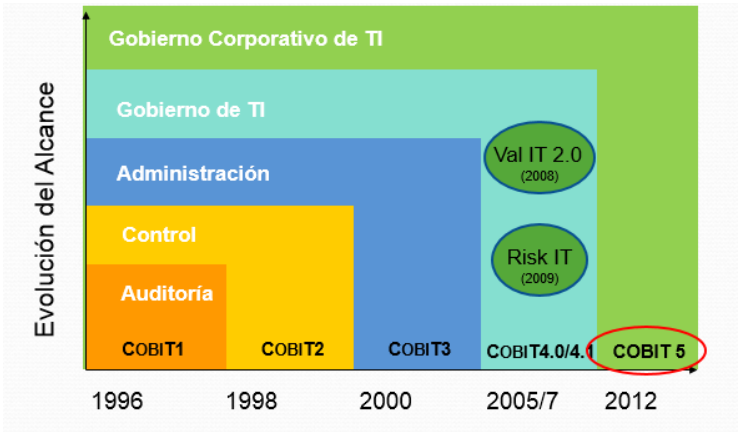

Figura 12. Evolución de COBIT
Fuente: Marco empresarial de ISACA, en www.isaca.org/cobit

Cobit 5 provee un marco de trabajo integral que ayuda a las empresas alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla,

ayuda a las empresas a crear el valor óptimo desde TI manteniendo equilibrio entre la generación de beneficios, optimización de los niveles de riesgo y el uso de recursos (ISACA, 2012b).

COBIT 5 permite a las tecnologías de la información ser gobernadas y gestionadas de un modo holístico para toda la empresa, de tal forma que de abarque al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, tomando en cuenta los intereses de las partes relacionadas tanto internas como externas a TI. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público (ISACA, 2012b).

Principios de Cobit 5

COBIT 5 se basa en cinco principios claves para el gobierno y la gestión de las TI empresariales que juntos habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas (ISACA, 2012b).

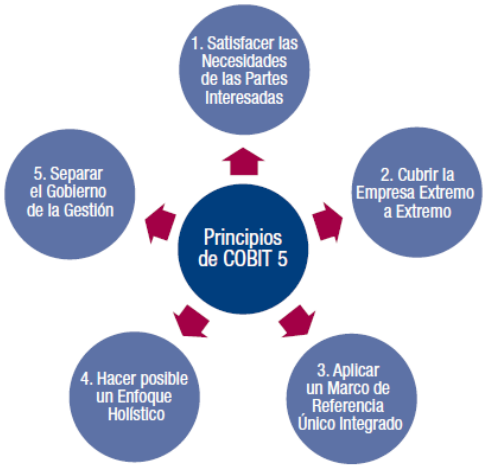

Figura 13. Principios de COBIT
Fuente: (ISACA, 2012)

1. Satisfacer las Necesidades de las Partes Interesadas. - Las empresas existen para crear valor para sus partes interesadas (accionistas), en consecuencia, cualquier empresa,

comercial o no, tendrá la creación de valor como un objetivo de Gobierno manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos (ISACA, 2012b).

2. Cubrir la Empresa Extremo a Extremo. - COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo, cubre todas las funciones y procesos dentro de la empresa; no se enfoca sólo en la "*función de TI*", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa (ISACA, 2012b).

3. Aplicar un marco de referencia único integrado. - COBIT 5 se alinea con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa (ISACA, 2012b).

4. Hacer posible un enfoque holístico. - COBIT 5 define un conjunto de catalizadores para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores son factores que individual y colectivamente se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. (ISACA, 2012b). El marco de trabajo COBIT 5 define siete categorías de catalizadores:

4.1 Principios, Políticas y Marcos de Trabajo
4.2 Procesos
4.3 Estructuras Organizativas
4.4 Cultura, Ética y Comportamiento
4.5 Información
4.6 Servicios, Infraestructuras y Aplicaciones
4.7 Personas, Habilidades y Competencias

5. Separar el Gobierno de la Gestión. - COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos (ISACA, 2012b).

La visión de COBIT 5 en esta distinción clave entre gobierno y gestión es:

Gobierno: asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

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

Procesos de COBIT 5

COBIT 5 no es prescriptivo, pero sí defiende que las empresas implementen procesos de gobierno y de gestión de manera que las áreas fundamentales estén cubiertas (ISACA, 2012b).

ISACA (2012b) divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos de COBIT 5:

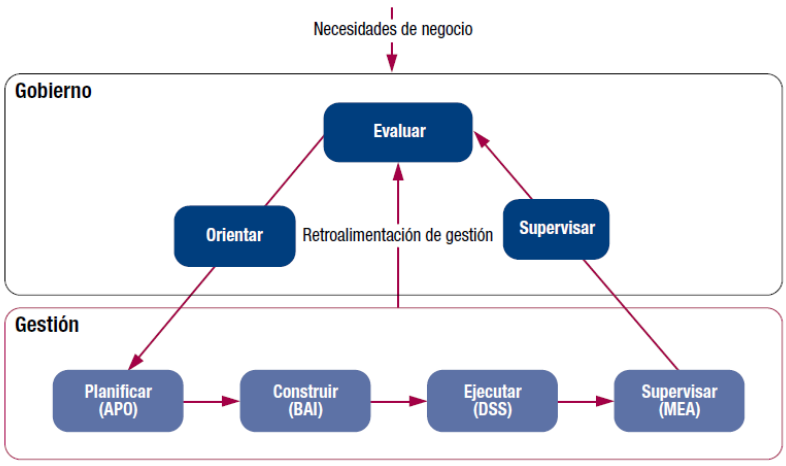

Figura 14. Áreas Clave de Gobierno y Gestión de COBIT 5
Fuente: (ISACA, 2012)

• *Gobierno.* - Contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (**EDM**).

• *Gestión.* - Contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (Plan, Build, Run and Monitor - PBRM), y proporciona cobertura de extremo a extremo de las TI. Los nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales:

- Alinear, Planificar y Organizar (Align, Plan and Organice, **APO**)
- Construir, Adquirir e Implementar (Build, Acquire and Implement, **BAI**)
- Entregar, dar Servicio y Soporte (Deliver, Service and Support, **DSS**)
- Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, **MEA**) (ISACA, 2012b)

El gobierno y gestión de los procesos COBIT 5, (ISACA, 2012b) aseguran que las empresas organizan sus actividades relacionadas con TI de un modo repetible y confiable. El modelo de referencia de proceso de COBIT 5, está conformado por cinco dominios y 37 procesos:

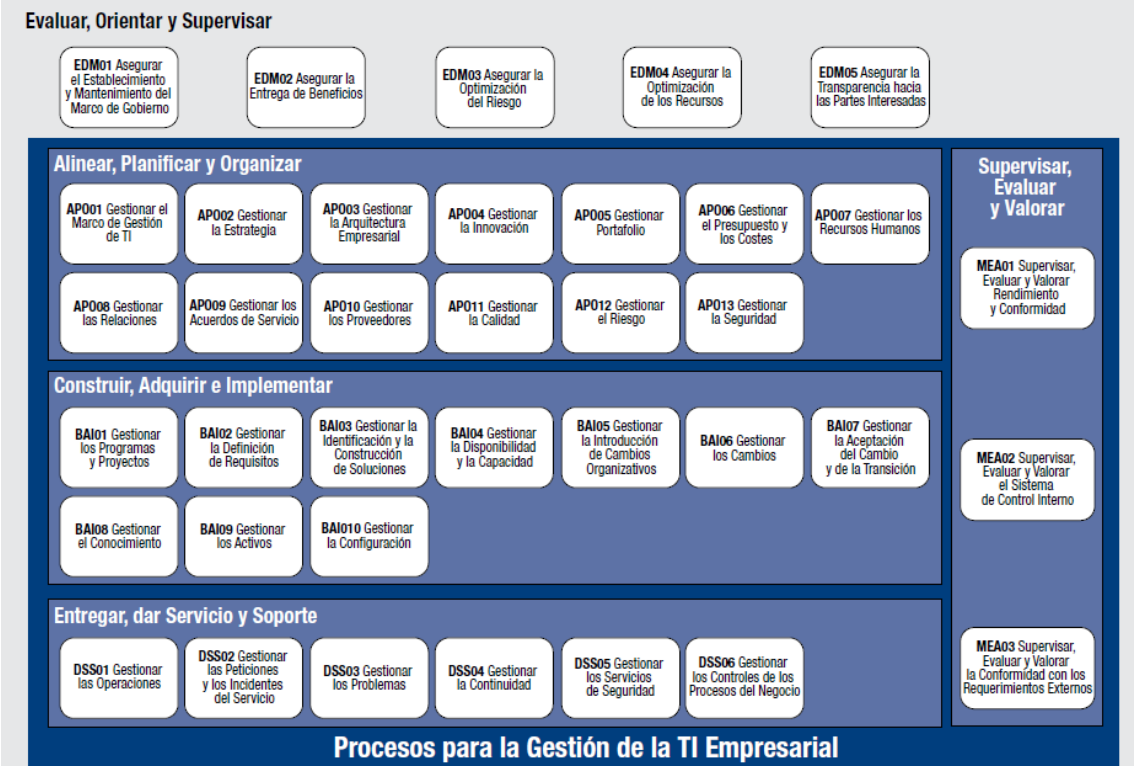

Figura 15. Procesos de Gobierno de TI Empresaria
Fuente: (ISACA,2012)

El modelo de referencia de COBIT 5 consolida COBIT 4.1, Val IT y Risk IT en un solo marco de referencia, y ha sido actualizado para alinearse con las mejores prácticas (ISACA,

2013), permitiendo de esta manera, que al utilizar COBIT 5 se aplique a su vez las mejores prácticas propuestas por Val IT y Risk IT.

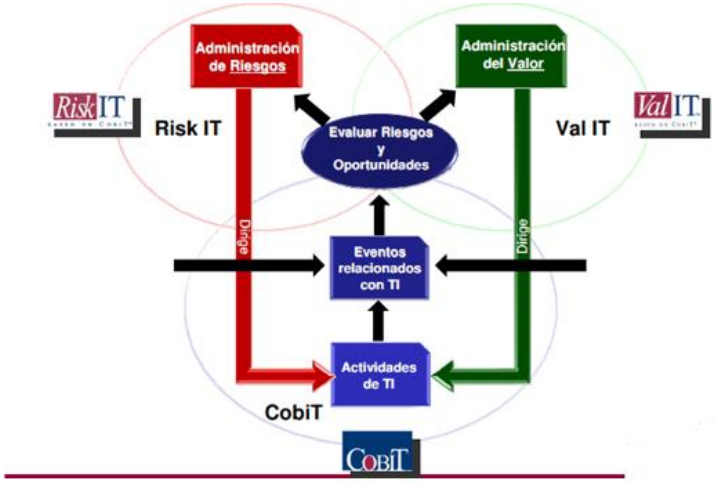

Figura 16. Modelo de Referencia
Fuente: Isaca Capítulo Monterrey Presentado por Gustavo A. Solís, (ISACA, 2009a)

COBIT 5 e ITIL v3 tienen procesos comunes y a su vez están diseñados pensando en el ciclo de vida de las aplicaciones, sistemas y servicios de TI; COBIT, ITIL e ISO-27000 contemplan ciclos de mejora continua; COBIT e ISO-27000 consideran controles enfocados a la seguridad de la información.

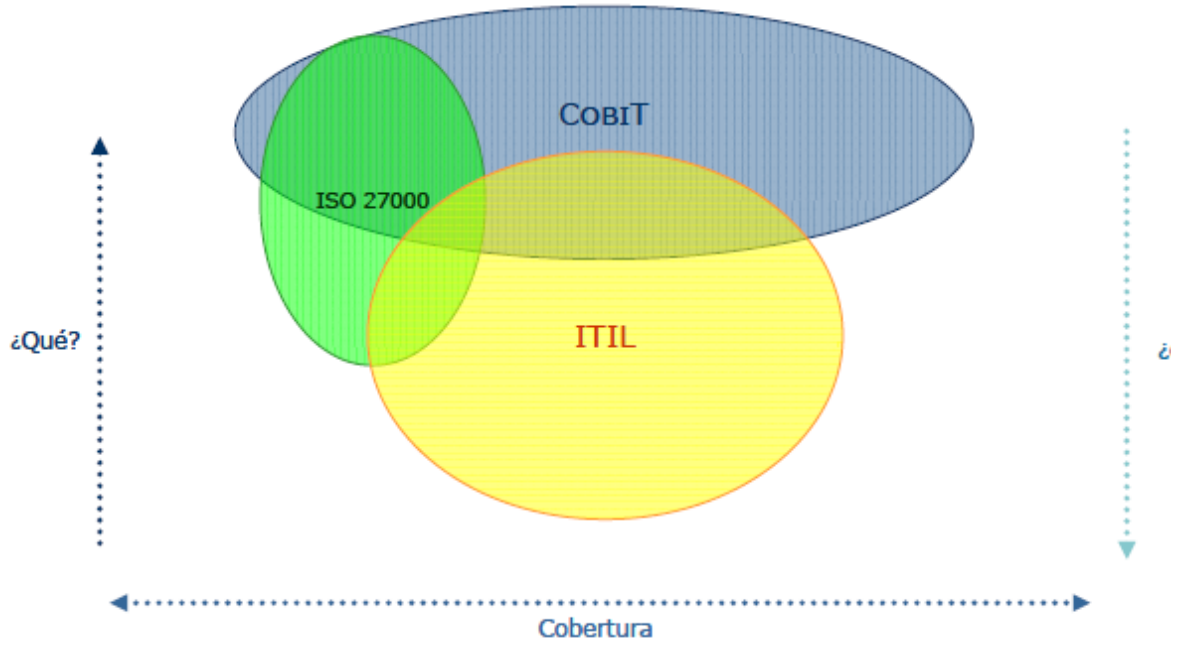

Figura 17. Procesos comunes
Fuente: Scitum, Héctor Acevedo Juárez

Las últimas versiones de cada uno de los marcos de referencia tomaron en cuenta a sus predecesores para contar con una mejora alineación.

2.2 RESUMEN ANÁLISIS DE ESTÁNDARES INTERNACIONALES, MARCOS DE TRABAJO Y MEJORES PRÁCTICAS

Tabla 15:

Estándares internacionales, marcos de trabajo y mejores prácticas

Referencia	Definición	Enfoque	Objetivos	Controles
COBIT 5	Control Objetives for Information and related Techonologies	Objetivos de control y gobierno de TI	Proveer un modelo de procesos con objetivos para asegurar la alineación de TI al negocio	Dominios: 5 Subdominios: 37 Controles: 210
COSO	Committee of Sponsoring Organizations of the Treadway Commission	Diseño, implementación, conducción del control interno y evaluación de su efectividad	Proporcionar una garantía razonable sobre el logro de objetivos de operaciones, reportes y cumplimiento	Componentes: 5 Principios: 20
ISO 27002	Organización Internacional de Normalización	Guía de buenas prácticas para mejorar la gestión de la seguridad de la información en una organización	Describir los objetivos de control y los controles para iniciar, implementar, mantener y la gestión de la seguridad de la información en una organización	Dominios: 14 Objetivos de control: 35 Controles: 114
ITIL	Information Technology Infraestructure	Mejores prácticas para la entrega de los servicios de Tecnología	Descripción de las mejores prácticas para la entrega de los servicios de Tecnología Informática con alta calidad y eficiencia	Fases: 5 Subprocesos: 23 Actividades: 148
VAL IT	Gobernance of IT Investment	Modelo de procesos para el gobierno de las inversiones de TI	Complementar la visión de COBIT desde el punto de la gestión financiera de las inversiones y costos de TI	Dominios: 3 Procesos: 22 Prácticas claves: 40
RISK IT	Gobernance of IT Risks	Modelo de procesos para el gobierno de los riesgos de TI	Asegurar que la gestión de riesgos de TI se integra con la gestión del riesgo corporativo	Ámbitos: 3 Procesos: 6 Actividades: 43
ISSAIs	International Standards of Supreme Audit Institutions	Marco de Normas Profesionales para las Entidades Fiscalizadoras Superiores	Promover una auditoría independiente y eficaz dentro de las Entidades Fiscalizadoras Superiores	Medidas de seguridad: 7

Nota: Elaborada por los autores, Figueroa F., Hinojosa L.

CAPÍTULO III

PROPUESTA DE NORMATIVA BASADA EN COBIT, PARA EL CONTROL INTERNO DE TECNOLOGÍAS DE LA INFORMACIÓN

El control interno de las entidades del sector público ecuatoriano se realiza con las Normas de Control Interno emitidas por la Contraloría General del Estado en el año 2009, mismas que en materia de tecnologías de la información y comunicaciones no han sido reformadas; por lo que en la actualidad se genera un vacío legal en el momento de generar una responsabilidad y no existe un apalancamiento legal de cumplimiento obligatorio con el que se puedan establecer recomendaciones de prevención, corrección y mejora.

La Constitución de la República del Ecuador publicada en Registro Oficial de 20 de octubre de 2008, en la tercera sección "Contraloría General del Estado", estableció:

"... Art. 211.- La Contraloría General del Estado es un organismo técnico encargado del control de la utilización de los recursos estatales, y la consecución de los objetivos de las instituciones del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos"

"... Art. 212.- Serán funciones de la Contraloría General del Estado, además de las que determine la ley: 1. Dirigir el sistema de control administrativo que se compone de auditoría interna, auditoría externa y del control interno de las entidades del sector público y de las entidades privadas que dispongan de recursos públicos. 2. Determinar responsabilidades administrativas y civiles culposas e indicios de responsabilidad penal, relacionadas con los aspectos y gestiones sujetas a su control, sin perjuicio de las funciones que en esta materia sean propias de la Fiscalía General del Estado..."

Artículos que fueron reformados por la Asamblea Nacional del Ecuador en sesión del 3 de diciembre de 2015 y publicada en el Suplemento del Registro Oficial 653, del 21 de noviembre de 2015 donde se aprobaron enmiendas constitucionales; con las que en los artículos 211 y 212 se suprimieron las frases "*y la consecución de los objetivos de las instituciones del Estado*" así como "*y gestiones*" retirando de esta manera a la Contraloría General del Estado la potestad de realizar revisiones de cumplimiento de objetivos institucionales; por lo que, en la Propuesta de Normativa basada en COBIT para el Control Interno de Tecnologías de la Información del sector Público Ecuatoriano no constarán controles relacionados con la gestión orientada al cumplimiento de objetivos de la entidad.

Una vez que en el capítulo anterior fueron analizados y comparados varios marcos de referencia con COBIT 5, mediante matrices comparativas se pueden desarrollar los controles idóneos y aplicables en las instituciones del sector público ecuatoriano tomando como referencia los controles de los estándares analizados apegados a la realidad de nuestro país.

Los controles se dividirán de acuerdo a los 5 dominios de Cobit de la siguiente manera:

3.1 Evaluar, Orientar y Supervisar (EOS)

Este dominio está formado por 5 procesos gobernantes y en cada uno se definen prácticas de evaluación, orientación y supervisión cuya meta es que los objetivos de la entidad sean alcanzados, mediante la optimización de riesgos y recursos valorando las necesidades de los interesados.

3.1.1 EOS01 Establecer y mantener el marco de Gobierno

La unidad de Tecnología de la Información analizará y articulará los requerimientos para el gobierno de TI de la institución; y pondrá en marcha y mantendrá firmes las estructuras, los

procesos y las prácticas, tendiendo claras las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la entidad.

EOS01.01 Evaluar el sistema de gobierno. - Identificará y en conjunto con las partes interesadas de la institución, documentará la que se comprendió de los requerimientos; y realizará una estimación del diseño actual y futuro del gobierno de TI de la entidad (organismo del sector público).

Analizará e identificará los factores del entorno (obligaciones legales, contractuales y regulatorias) y tendencias en el entorno del negocio que pueden influir en el diseño del gobierno, determinará la relevancia de TI y su papel con respecto al negocio, alineará el uso y el procesamiento ético de la información con los objetivos, visión y dirección de la entidad y determinará las implicaciones del entorno de control conjunto de la entidad con respecto a TI.

EOS01.02 Dirigir el sistema de gobierno de TI. - Informará y solicitará a los líderes apoyo y aceptación, guiará las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno, definirá la información necesaria para una toma de decisiones informadas.

Establecerá estructuras, procesos y prácticas del gobierno alineados con los principios de diseño acordados; asignará responsabilidad y autoridad para que se apliquen los principios de diseños de gobierno y los modelos de toma de decisiones; orientará al personal para que siga las directrices relevantes para un comportamiento ético y profesional; garantizará que las consecuencias del no cumplimiento se conozcan; y establecerá un sistema de recompensa para promover el cambio cultural.

EOS01.03 Supervisar el sistema de gobierno. - Supervisará la ejecución y la efectividad del gobierno de TI de la entidad, analizará si el sistema de gobierno y los mecanismos

implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI.

Evaluará la efectividad y rendimiento de las partes interesadas en las que se ha delegado responsabilidad para el gobierno de TI de la entidad; evaluará periódicamente si los mecanismos para el gobierno de TI están establecidos y operan efectivamente; y revisar los mecanismos frecuentes para garantizar que el uso de las tecnologías de la información cumple con las regulaciones importantes (regulatorias, legislación, leyes comunes, contractuales), estándares y directrices.

3.1.2 EOS02 Aseverar la Entrega de Beneficios

La unidad de Tecnología de la Información optimizará la contribución al valor del negocio desde los procesos del negocio, asegurando un valor óptimo de inversión hecha para los servicios TI y activos de TI.

EOS02.01 Evaluar la optimización de valor. –Evaluará periódicamente las inversiones, servicios y activos orientados al cumplimiento de los objetivos de la entidad a un costo razonable.

Comprenderá los pedidos de los interesados, temas como la dependencia de las tecnologías de la información y sus capacidades; verificará los elementos claves de gobierno necesarios para la entrega confiable, segura y a un valor óptimo por el uso de los servicios, activos y recursos de TI existentes; y considerará evaluar la efectividad de los roles, responsabilidades y asignaciones para la toma de decisiones respecto a las inversiones, servicios y activos de TI.

EOS02.02 Dirigir y supervisar la optimización del valor. –Orientará y supervisará los principios y prácticas para posibilitar la optimización de los costos de las inversiones TI a lo largo de todo su ciclo de vida económico.

Definirá y comunicará los tipos de inversión, categorías, criterios y ponderaciones relativas a los criterios que permitan puntuaciones de valores relativos; considerará usos potenciales de TI innovadores que posibiliten que la entidad responda a nuevas oportunidades y desafíos, incremente la competitividad o mejore sus procesos; recomendará la consideración de innovaciones potenciales, cambios organizativos o mejoras operativas que desde las iniciativas TI pudieran impulsar un incremento de valor para la entidad; recogerá los datos pertinentes, oportunos, completos, fiables y precisos para informar sobre los avances en la entrega de valor; y tomará las medidas apropiadas para asegurar que el valor sea optimizado.

3.1.3 EOS03 Asegurar la Optimización del Riesgo

La unidad de Tecnología de la Información asegurará que el riesgo para el valor de la entidad relacionado con el uso de las TI sea identificado y tratado de manera que la tolerancia al riesgo de la entidad sea entendida y comunicada.

EOS03.01 Evaluar el control de riesgos. –Evaluará periódicamente el efecto del riesgo sobre el uso actual y futuro de TI en la entidad.

Analizará si el riesgo relacionado con el uso de TI es identificado y tratado; evaluará propuestas de umbrales de tolerancia al riesgo de TI frente a los niveles de riesgo y oportunidad aceptables por la entidad; y observará las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la entidad para las pérdidas relacionadas con TI.

EOS03.02 Orientar al control de riesgos. –Establecerá prácticas de control de riesgos para proporcionar una seguridad razonable del riesgo de TI.

Impulsará el aprendizaje sobre los riesgos de TI y estimulará a la entidad a identificar proactivamente los riesgos tecnológicos, las oportunidades y los potenciales impactos en la entidad, de manera que operaciones y la estrategia de riesgos de TI estén integradas con las

decisiones y operaciones estratégicas de la entidad; implantará mecanismos apropiados para responder rápidamente a los riesgos cambiantes; identificará los objetivos e indicadores clave de los procesos control de riesgos a ser monitorizados y aprobará los métodos, técnicas y procesos para capturar y notificar la información de medición.

EOS03.03 Supervisar la gestión de riesgos. –Supervisará los objetivos y las métricas clave de los procesos de control de riesgo y establecerá cómo las desviaciones y problemas serán identificados, seguidos e informados para su resolución.

Supervisará las metas y métricas clave de control de los procesos de gobierno y control del riesgo respecto a los objetivos, analizará las causas de las desviaciones y tomará medidas correctivas; e informará cualquier problema de control de riesgos.

3.1.4 EOS04 Asegurar la Optimización de los Recursos

La unidad de Tecnología de la Información asegurará que las capacidades relacionadas a TI (personas, procesos y tecnologías) sean adecuadas, suficientes y estén disponibles para soportar eficazmente los objetivos de la entidad a un costo óptimo.

EOS04.01 Valorar la administración de recursos. –Calculará consecutivamente la necesidad de recursos tecnológicos, la posible asignación de ellos y los principios que deben cubrir las necesidades de la entidad.

Examinará las opciones de abastecimiento de recursos tecnológicos y buscará cubrir los requerimientos de la entidad; definirá principios para la designación de recursos para que TI pueda satisfacer los requisitos de la entidad; revisará y aprobará el plan de recursos y las estrategias de arquitectura de la institución para la entrega de valor y la mitigación de riesgos con los recursos asignados.

EOS04.02 Dirigir y supervisar la administración de recursos. –Implementará y supervisará la adopción de principios de administración de recursos para brindar un uso óptimo de los recursos de TI a lo largo de su completo ciclo de vida económica.

Impulsará y controlará la adopción de estrategias de asignación de recursos, responsabilidades, principios y el plan de recursos y las estrategias de arquitectura de empresa; definirá y supervisará los objetivos, medidas y métricas clave para la gestión de los recursos.

3.1.5 EOS05 Asegurar la Transparencia hacia las partes interesadas

La unidad de Tecnología de la Información asegurará que los informes en cuanto a desempeño de TI de la entidad son transparentes y cuentan con la aprobación de los interesados.

EOS05.01 Evaluar los requisitos de elaboración de informes. –Examinará continuamente los requisitos de comunicación con las partes interesadas para la elaboración de informes respecto al uso de TI en la entidad, incluyendo requisitos obligatorios de elaboración de informes, así como la comunicación a otros interesados (alcance y frecuencia).

Mantendrá la comunicación con los interesados tanto externos como internos, a través de formatos y conductos de comunicación, así como los principios de aceptación y aprobación de los informes por parte de los interesados.

EOS05.02 Dirigirá y supervisará la comunicación con las partes interesadas y la elaboración de los informes. –Establecerá y supervisará una estrategia de comunicación y una elaboración de informes eficaces, con mecanismos de aseguramiento de calidad y completitud de la información.

Implementará y supervisará mecanismos de cumplimiento de precisión y fiabilidad en cuanto a elaboración de informes de TI; y evaluará periódicamente la eficacia de los mecanismos de comunicación y la entrega de informes.

3.2 Alinear, Planificar y Organizar (APO)

Este dominio contiene 13 procesos que cubren las estrategias y las tácticas que permiten identificar la forma en que la Dirección de Tecnologías de la Información contribuye con los objetivos de la entidad; es decir, proporciona la dirección para la entrega de soluciones y servicios.

3.2.1 APO01 Administrar el marco de gobierno de TI

La unidad de Tecnología de la Información definirá y mantendrá el gobierno de la misión y la visión corporativa de TI. Implementará mecanismos y responsables para la gestión de la información y el uso de TI en la entidad apoyando los objetivos de gobierno conforme las políticas definidas.

APO01.01 Establecer la estructura de la organización. - Desarrollará una estructura interna para la organización que manifieste las necesidades de la entidad y las prioridades de la Dirección de TI. Implementará comités para que las decisiones sean tomadas de forma más eficaz y eficiente.

La unidad de tecnología de información, formará parte de la estructura organizacional de la institución en un nivel donde pueda ejecutar tareas de apoyo y asesoría tanto a las autoridades como a las unidades usuarias; además participará en la toma de decisiones de la entidad y generación de cambios para la mejora tecnológica mediante el establecimiento de un Comité Estratégico de TI que se definirá según el tamaño y complejidad de la entidad y vigilará que el gobierno de TI, como parte del gobierno corporativo, sea visto de forma adecuada, aconseje sobre la dirección estratégica, revise las inversiones, realice seguimiento del estado de los proyectos y resuelva los conflictos de recursos, supervise los niveles de servicio y las mejoras en el servicio; y se establecerán las funciones, atribuciones, personal implicado y responsabilidades del Comité

Estratégico de TI para la toma de decisiones, (quiénes rendirán cuentas, responsables, consultados e informados).

APO01.02 Establecer roles y responsabilidades. – Establecerá y comunicará roles y responsabilidades del personal de TI, que reflejen claramente las necesidades del negocio y los objetivos de TI, la seguridad de la información, así como las responsabilidades y la rendición de cuentas para la aprobación y toma de decisiones.

Definirá los roles y responsabilidades considerando que un solo rol no controle un proceso crítico, y garantizará una adecuada segregación de funciones, para evitar un uso inadecuado o funciones incompatibles e incluirá en las descripciones las políticas y los procedimientos definidos y prácticas profesionales; adicionalmente se tomará en cuenta la definición de políticas y medidas de soporte de seguridad para accesos a distancia.

APO01.03 Mantener actividades de cumplimiento y mejora continua. – Implementará una comunicación clara de expectativas/requisitos, fomentará la cooperación entre departamentos y el trabajo en equipo, promoverá el cumplimiento y la mejora continua.

Integrará los principios de tecnología con los principios de la entidad; alineará los controles de la Dirección de TI con el entorno de políticas tecnológicas, marcos de trabajo de gobierno de TI y procesos de tecnología, que cumplan con los objetivos de control tecnológicos incluyendo calidad, seguridad, confidencialidad, control interno, e implementará normas para el uso de activos tecnológicos; y evaluará buenas prácticas disponibles, como el Marco de Trabajo Integrado para Control Interno de COSO, especificará, documentará y divulgará las políticas, estándares y procedimientos que normen las tareas concernientes a tecnología de la información y comunicaciones en la entidad y los actualizará y revisará de forma periódica.

APO01.04 Comunicar los objetivos y la dirección de TI. –Comunicará la sensibilización y la comprensión de los objetivos y la dirección de TI a las partes interesadas y usuarios pertinentes a lo largo de toda la entidad.

Comunicará periódicamente los objetivos y la dirección de TI, con una clara definición de la misión, los objetivos de servicio, seguridad, controles internos, políticas y procedimientos, roles y las responsabilidades asegurando que las comunicaciones reciban apoyo de las autoridades correspondientes.

APO01.05 Optimizar la ubicación de la función de TI. –Posicionará la unidad de TI en la estructura organizativa global para reflejar la importancia de TI en la organización, su criticidad y el nivel de dependencia de TI.

APO01.06 Definir la propiedad de la información (datos) y del sistema. –Definirá y comunicará las responsabilidades de la propiedad de la información (datos) y los sistemas de información, asegurará que los propietarios toman decisiones acuerdes a la clasificación de la información y los sistemas y su protección.

Proveerá políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información (datos) en la entidad; definirá e implementará procedimientos para asegurar la integridad y consistencia de toda la información almacenada en formato electrónico, tales como bases de datos, almacenes de datos (data warehouse) y archivos de datos; implementará herramientas, técnicas y directrices para mantener un control efectivo y la seguridad sobre los datos y aplicaciones instaladas o utilizadas con los responsables de la entidad; y precisará un inventario de la información con los propietarios y custodios.

APO01.07 Administrar la mejora continua de los procesos. –Evaluará, planificará y ejecutará la mejora continua de procesos.

Identificará los procesos críticos de la entidad a través de un análisis del rendimiento, del cumplimiento y de los riesgos afines; identificará opciones de mejora y reingeniería de procesos desarrollando métricas de rendimiento para supervisar las mejoras; y aplicará prácticas de gestión de calidad para la actualización de procesos y mejora de eficiencia y eficacia (mediante formación, documentación, estandarización y automatización de procesos).

APO01.08 Mantener el cumplimiento con las políticas y procedimientos. –Pondrá en ejecución procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y actividades aprobadas por la máxima autoridad de la institución; y aplicará acciones apropiadas al no cumplimiento o desempeño inadecuado.

Evaluará periódicamente el cumplimiento de políticas y actividades por parte de los empleados y de personas externas; e integrará rendimiento y cumplimiento dentro de los objetivos individuales del personal.

3.2.2 APO02 Administrar la estrategia

La unidad de Tecnología de la Información proporcionará una visión completa del negocio actual y del entorno de TI, su dirección futura, y las iniciativas para migrar al entorno deseado. Aprovechará los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos del negocio.

APO02.01 Comprender la dirección de la entidad. – Definirá el entorno actual y los procesos de negocio de la entidad, así como la estrategia de la entidad y sus retos operativos.

Identificará las partes interesadas y obtendrá comprensión de sus requerimientos, analizará los cambios en la entidad y determinará prioridades para los cambios estratégicos contando con la aprobación de la máxima autoridad.

APO02.02 Evaluar el entorno, capacidades y rendimiento actuales. – Evaluará el rendimiento del negocio, las capacidades de TI y los servicios externos de TI, identificará los problemas que se están experimentando y generará recomendaciones que detallen beneficios.

Desarrollará un punto de referencia del negocio, entorno de TI, capacidades y servicios actuales de manera que las necesidades futuras puedan ser comparadas; identificará los problemas, fortalezas, oportunidades y amenazas en el entorno existente, las capacidades y servicios para entender el desempeño actual y tender a mejorar en términos de la contribución de TI a los objetivos del negocio; evaluará el impacto de posibles cambios en el negocio y en los modelos operativos de TI, la capacidad de investigación y desarrollo de tecnología y los programas de inversión de TI.

APO02.03 Definir el plan estratégico. – Elaborará un plan informático estratégico para administrar los recursos tecnológicos, el mismo que deberá estar alineado con el plan estratégico institucional, que defina la contribución a los objetivos estratégicos de la entidad. Incluyendo cómo TI apoyará el programa aprobado de inversiones, procesos de negocio, servicios y activos de TI.

El plan informático estratégico tendrá un nivel de detalle suficiente para permitir la definición de planes operativos de tecnología de Información y especificará como ésta contribuirá a los objetivos estratégicos de la organización; incluirá un análisis de la situación actual y las propuestas de mejora con la participación de todas las unidades de la entidad.

Definirá los procedimientos para migrar del entorno que se tiene en la actualidad al propuesto, tomando en cuenta el presupuesto, las fuentes de financiamiento y la estrategia de abastecimiento; identificará los costos, riesgos e implicaciones de realizar cambios en la organización, el desarrollo tecnológico, los requisitos legales, la reingeniería de procesos de la entidad, el personal, la oportunidades de contratar servicios externos; y obtendrá formalmente soporte de las partes interesadas y tramitará la aprobación del plan.

3.2.3 APO03 Administrar la arquitectura de la entidad

La unidad de Tecnología de la Información establecerá una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica; definirá los requisitos, normas, directrices, procedimientos, plantillas y herramientas que proporcionen un vínculo entre estos componentes; y mejorará la agilidad y calidad de la información, mediante iniciativas de reutilización de bloques de componente.

APO03.01 Desarrollar la visión de la arquitectura. – Definirá una visión de la arquitectura a alto nivel cubriendo los dominios de negocio, información, datos, aplicaciones y tecnología; describirá como nuevas capacidades permitirán alcanzar las metas de la entidad y los objetivos estratégicos.

Identificará las partes interesadas claves de la entidad, objetivos y preocupaciones; definirá los requisitos claves de la entidad a ser considerados, incluirá los objetivos y los impulsores estratégicos de la empresa y considerará las limitaciones de la entidad y específicas del proyecto (duración, planificación, recursos, etc.)con las que habrá que tratar, entenderá los objetivos estratégicos de la entidad; y trabajará conjuntamente con la planificación estratégica para asegurar que las oportunidades de arquitectura de TI empresarial se apoyan en el desarrollo del plan estratégico.

APO03.02 Definir la arquitectura de referencia. – Describirá la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.

Mantendrá un repositorio de la arquitectura que contenga los estándares, los componentes reutilizables, el modelado, las relaciones, las dependencias y las vistas para permitir uniformidad y mantenimiento; conservará un modelo de arquitectura de procesos; generalizará la documentación de los procesos; y definirá las funciones y responsabilidades de los propietarios, usuarios y cualquier otra parte interesada en el proceso.

La arquitectura de información contendrá el modelo de información de la entidad que facilite el desarrollo, uso y compartición de la misma, de forma que garantice su integridad, disponibilidad, seguridad y exactitud, para permitir un uso óptimo de la información para la toma de decisiones; y conservará un diccionario de datos documental y actualizado que incluya detalles sobre el propietario de los datos, definición de los niveles de seguridad apropiados y los requisitos de retención y destrucción de los datos, las reglas de validación, controles de integridad y consistencia.

APO03.03 Definir la implementación de la arquitectura. – Definirá un plan de implementación y migración razonable según la cartera de proyectos y programas, considerando recursos disponibles y necesarios para finalizar los trabajos.

Establecerá lo que deberían incluir el plan de implementación y migración formando parte del programa y plan de proyectos para asegurarse que están alineados con los requisitos; y corroborará las fases y las mantendrá actualizadas en el documento de la arquitectura.

APO03.04 Suministrar los servicios de arquitectura empresarial. – Establecerá servicios de arquitectura empresarial a través de la supervisión de los proyectos que serán implementados.

Orientará sobre el alcance y las prioridades de las soluciones que se desplegarán; tratará la cartera de servicios con el fin de asegurar que se ajustan a los objetivos estratégicos de la entidad y el desarrollo de soluciones; y brindará soporte con los principios de dicha arquitectura, modelos y componentes básicos.

3.2.4 APO04 Administrar la innovación

La unidad de Tecnología de la Información identificará las oportunidades de innovación y planificará la innovación en relación con las necesidades del negocio. Analizará oportunidades de mejora que puede crearse basado en nuevas tecnologías, servicios, así como por la innovación en procesos empresariales y de TI.

APO04.01 Crear un entorno favorable para la innovación. – Creará un entorno que sea propicio para la innovación, que considere foros tecnológicos y mecanismos para promover y captar ideas de los empleados.

Definirá un plan de innovación que incluya administración de riesgos y presupuesto; proveerá una infraestructura que pueda permitir innovar; considerará herramientas de colaboración para mejorar el trabajo entre diferentes ubicaciones geográficas y divisiones de la entidad; elaborará un programa que permita a los servidores presentar ideas innovadoras; y creará una estructura adecuada de toma de decisiones para evaluar y aplicar estas ideas.

APO04.02 Conservar la comprensión del entorno de la entidad. – Trabajará con los interesados para entender sus retos, de modo que las oportunidades habilitadas por las nuevas tecnologías puedan ser identificadas.

Entenderá el negocio y a la entidad con sus operaciones de modo que los potenciales valores añadidos tecnológicos o innovaciones TI puedan ser identificadas; realizará reuniones periódicas con las unidades de negocio, y/o otras entidades interesadas para entender los problemas actuales del negocio, cuellos de botella de los procesos u otras limitaciones donde la innovación TI puede crear oportunidades.

APO04.03 Supervisar y explorar el entorno tecnológico. –Realizará una supervisión del entorno externo a la entidad para identificar tecnologías que tengan el potencial de optimizar tiempos y costos, evitando la obsolescencia y mejorando los procesos corporativos y de TI.

Realizará estudios y analizará el mercado, incluyendo sitios web apropiados, diarios y conferencias para identificar tecnologías emergentes que automaticen las diligencias interinstitucionales y ciudadanos, y definirá procedimientos para su utilización; recopilará las ideas innovadoras del personal de TI y las analizará para su posible implementación, incluyendo seguridades como el uso de firma electrónica para el intercambio de información entre instituciones mediante el uso de archivos digitales a los que se pueda aplicar este tipo de control.

APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras. –Analizará las sugerencias y tecnologías innovadoras identificadas trabajando con las partes interesadas para validar las suposiciones sobre el potencial de las nuevas tecnologías y la innovación, por ejemplo, tecnología que permitiría innovar el trabajo desde otro lugar que no sea la oficina.

Evaluará las tecnologías identificadas, considerando aspectos tales como tiempo para alcanzar la madurez, riesgo inherente de la nueva tecnología, posibles implicaciones legales; identificará cualquier problema que pueda necesitar ser resuelto o probado a través de una iniciativa de prueba de concepto; obtendrá autorización para realizar pruebas de concepto y las

realizará evaluando las tecnologías emergentes u otras ideas innovadoras; e identificará cualquier problema y determinará si más implementaciones deberían ser tenidas en cuenta, basándose en la viabilidad y el potencial retorno de la inversión (ROI).

APO04.05 Recomendar iniciativas apropiadas adicionales. –Evaluará y supervisará los resultados de las pruebas de concepto, generar recomendaciones para más iniciativas y obtendrá el soporte de las partes interesadas.

Documentará los resultados de las pruebas de concepto favorables y no favorables; e incluirá recomendaciones de innovación y tendencias, e informará sobre las oportunidades de descubrimientos viables.

APO04.06 Supervisar la implementación y el uso de la innovación. –Supervisará la implementación y uso de las tecnologías emergentes durante la integración y adopción para garantizar que se producen los beneficios prometidos.

Documentará las lecciones aprendidas y oportunidades de mejora, y evaluará el posible valor obtenido a través de la innovación.

3.2.5 APO05 Administrar el portafolio

La unidad de Tecnología de la Información identificará, evaluará, priorizará y equilibrará programas y servicios; gestionará la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos, así como en su valor y riesgo corporativo; supervisará el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.

APO05.01 Establecer la mezcla del objetivo de inversión. –Revisará y garantizará la claridad de las estrategias y servicios actuales corporativos y de TI, ajustará las estrategias corporativas y de TI cuando sea necesario.

Conseguirá un entendimiento común entre TI y otras funciones de negocio sobre las potenciales oportunidades de TI para garantizar que las inversiones de TI y sus servicios estén alineadas con la visión de la entidad.

APO05.02 Determinar la disponibilidad y las fuentes de fondos. –Determinará las posibles fuentes de fondos, opciones de financiación y las implicaciones de estas fuentes de financiamiento sobre las expectativas del retorno de inversión; mantendrá un control de la disponibilidad y el compromiso de los fondos actuales, el gasto actual aprobado y la cantidad real gastada hasta la fecha.

APO05.03 Evaluar y seleccionar los programas a financiar. –Evaluará y definirá prioridades en los casos de negocio de programas: y decidirá sobre las propuestas de inversión e iniciará los programas.

Realizará evaluaciones de los programas propuestos; verificará el alineamiento estratégico, beneficios corporativos, riesgo y disponibilidad de recursos; establecerá procedimientos para comunicar el costo, beneficios y aspectos relativos al riesgo de esos programas a los procesos de priorización.

APO05.04 Supervisar, mejorar e informar el rendimiento del portafolio. – Periódicamente supervisará el rendimiento del portafolio de inversiones y de los programas individuales a lo largo de todo el ciclo de vida de inversión con capacidades de TI apropiadas.

Verificará continuamente el portafolio para eliminar programas duplicados e identificar y mitigar el riesgo, cuando sucedan cambios; volverá a evaluar y a priorizar el portafolio para

asegurar que está alineado con la estrategia del negocio; desarrollará métricas para medir la contribución de TI a la entidad respecto a los beneficios obtenidos; establecerá objetivos de rendimiento adecuados que reflejen las metas de capacidad corporativas y de TI; e implementará acciones correctivas cuando los beneficios alcanzados se desvíen significativamente de los esperados.

3.2.6 APO06 Administrar los recursos humanos

La unidad de Tecnología de la Información garantizará una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos, mediante comunicación clara de funciones y responsabilidades definidas, formación y planes de desarrollo personal y las métricas de desempeño.

APO06.01 Mantener dotación de personal adecuada y apropiada. –Evaluará las necesidades de personal en forma periódica o en cambios operativos asegurando que la entidad posee recursos humanos suficientes para apoyar las metas y objetivos de la entidad.

Mantendrá los procesos de contratación y de retención del personal de TI y del negocio acorde con las políticas y procedimientos de personal de la entidad; incluirá controles de antecedentes en el proceso de contratación de TI para empleados, contratistas y proveedores, considerando la criticidad de la función; realizará entrenamiento cruzado para reducir la dependencia de personal; y definirá los términos y condiciones para las contrataciones, incluirá responsabilidades respecto a la seguridad de la información.

APO06.02 Identificar personal, habilidades y competencias de TI. –Identificará el personal clave de TI; y reducirá la dependencia de personal en la realización de funciones críticas mediante la adquisición de conocimiento (documentación), intercambio de conocimientos, capacitación, planificación de la sucesión y respaldo del personal.

Identificará las necesidades tanto del personal de tecnología como de los usuarios funcionales y proporcionará una planificación de desarrollo profesional para fomentar el crecimiento de competencias según el puesto de trabajo, oportunidades de progreso personal y una menor dependencia de personas clave, concederá acceso a repositorios de conocimiento para apoyar el desarrollo de habilidades y competencias; mantendrá capacitación constante sobre seguridad de la información; y verificará los materiales y programas de formación de manera regular para asegurar su competitividad a los requisitos cambiantes y su impacto en los conocimientos, aptitudes y habilidades.

APO06.03 Evaluar el desempeño laboral de los servidores. –Evaluará de forma periódica el rendimiento del personal respecto a los objetivos individuales, responsabilidades específicas del trabajo y el marco de habilidades y competencias; así como el cumplimiento de normas y políticas establecidas, incluyendo las sanciones impuestas por el incumplimiento de las mismas.

Definirá un procedimiento para el uso y almacenamiento de información personal en el proceso de evaluación y sobre datos aplicables; retroalimentará de forma oportuna acerca del desempeño evaluado en relación a las metas del servidor y definirá planes de mejora del desempeño considerando los resultados del proceso de evaluación y los requisitos de capacitación de competencias identificados.

APO06.04 Realizar seguimiento del uso de recursos humanos de TI. –Identificará las carencias y proporcionará datos de entrada a los planes de aprovisionamiento, planes de abastecimiento de procesos de contratación del negocio y de TI y procesos de contratación del negocio y de TI.

Creará y actualizará de forma periódica un inventario de recursos humanos de TI; revisará la demanda actual y futura de recursos humanos para apoyar el logro de los objetivos de TI y ofrecer servicios y soluciones; y llevará control adecuada sobre el tiempo dedicado a diferentes tareas, trabajos, servicios o proyectos.

APO06.05 Instruir al personal de TI. –Asegurará que los consultores y el personal relacionado de TI conocen y cumplen las políticas de la entidad, así como leyes y reglamentos del sector público.

Definirá e implementará un acuerdo formal al cumplimiento obligatorio con el marco de control de TI de la entidad, tal como políticas de control de seguridad, control de acceso físico y lógico, uso de las instalaciones, requisitos de confidencialidad de la información, uso de certificados de firma digital, privacidad de la información de autenticación y los acuerdos de confidencialidad; revisará el trabajo de los contratistas y realizará su aprobación para los pagos basados en los resultados; examinará de forma periódica que el personal ha firmado y aceptado todos los acuerdos necesarios; y en el caso de certificados digitales solicitará la renovación o revocación del mismo según sea el caso.

3.2.7 APO07 Administrar los acuerdos de servicio

La unidad de Tecnología de la Información alineará los niveles de servicio de TI con las necesidades presentes y futuras de la entidad, incluyendo identificación, supervisión de los servicios TI, e indicadores de rendimiento.

APO07.01 Identificar servicios TI. –Analizará los requisitos del negocio y el modo en que los servicios TI y los niveles de servicio soportan los procesos del negocio; e identificará posibles servicios nuevos o modificaciones.

Valorará los servicios TI actuales y los niveles de servicio existentes, analizará, y estimará la futura demanda y confirmará la capacidad de los servicios TI existentes: identificará la necesidad de servicios TI nuevos o rediseñados; y revisará el catálogo de servicios TI regularmente para identificar servicios obsoletos.

APO07.02 Catalogar servicios de TI y definir acuerdo de servicio. –Definirá, priorizará y actualizará catálogos de servicios, publicará y mantendrá los servicios TI activos en los catálogos, definirá y preparará los acuerdos de servicio basándose en las opciones de los catálogos de servicio.

Analizará los requisitos para acuerdos de servicios nuevos o modificados recibidos; y considerará aspectos como tiempos del servicio, disponibilidad, rendimiento, capacidad, seguridad, continuidad, cumplimiento normativo, usabilidad y limitaciones.

APO07.03 Monitorear y reportar los niveles de servicio, acuerdos y contratos. – Establecerá procedimientos para supervisar y recopilar datos del nivel del servicio, proporcionará periódicamente informes del rendimiento de los servicios de TI, identificará tendencias y acordará planes de acción correctiva y de mejora para el desempeño y control de los incidentes o tendencias negativas.

Realizará revisiones periódicas de los acuerdos de servicio y cuando sea necesario, verificará los términos de los acuerdos de servicio de forma periódica para garantizar que en el tiempo son efectivos y actuales y que los cambios en los requisitos, servicios TI y niveles de servicio se tienen en cuenta de forma apropiada.

3.2.8 APO08 Administrar los proveedores

La unidad de Tecnología de la Información administrará los servicios de TI prestados por los proveedores, incluyendo la selección de proveedores, contratos, revisión y supervisión del desempeño, asegurando eficacia y cumplimiento adecuados.

APO08.01 Identificar y evaluar contratos. –Identificará proveedores y contratos, y establecerá un criterio de evaluación de los contratos actuales y alternativos con los proveedores.

Valorará y categorizará los proveedores y contratos existentes de acuerdo con criterios como tipo, relevancia y criticidad; mantendrá un detalle de proveedores que deben ser administrados cuidadosamente; evaluará y comparará periódicamente el rendimiento de los proveedores actuales y alternativos para identificar oportunidades de mejora con los proveedores actuales.

APO08.02 Seleccionar proveedores. –En casos que amerite escogerá proveedores de acuerdo con prácticas que aseguren la selección del que mejor se adapte a los requisitos.

Mantendrá evidencia documental de las evaluaciones realizadas a las ofertas de los proveedores; verificará las referencias de los proveedores candidatos, en el caso de adquisición de software, incluirá derechos (propiedad, licenciamiento, código fuente), en el caso de adquisición de infraestructuras, instalaciones y servicios relacionados; e incluirá controles (niveles de servicio) y en las obligaciones de todas las partes en los términos contractuales, mantenimiento, garantías, procesos de arbitraje, condiciones de actualización, seguridad, integridad, confidencialidad, garantías y derechos y controles de acceso.

APO08.03 Administrar contratos, cumplimiento y relación con proveedores. – Administrará y supervisará los contratos y la entrega de servicios; y asignará propietarios y responsables de las relaciones, calidad del servicio y cumplimiento contractual para cada

proveedor; así como aplicación de acuerdos de confidencialidad, requisitos de seguridad y nivel de servicios con cada proveedor.

Definirá procedimientos para tratar los conflictos contractuales haciendo uso primero, siempre que sea posible, de relaciones y mecanismos de comunicación eficaces que permitan superar los problemas de servicio; y supervisará y revisará el cumplimiento de la entrega de servicios asegurando una calidad del servicio adecuada, cumplimiento de los requisitos y las condiciones de los contratos.

3.2.9 APO09 Administrar la calidad

La unidad de Tecnología de la Información definirá requisitos de calidad en todos los procesos y procedimientos incluyendo controles y prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.

APO09.01 Establecer un sistema de gestión de la calidad. –Definirá un SGC que proporcione calidad para la información, tecnología y procesos de negocio de forma que incluya un enfoque continuo, estandarizado, formal y que esté alineado con los requerimientos del negocio.

Definirá roles, tareas, capacidades de decisión y responsabilidades para la gestión de la calidad; supervisará y medirá la eficacia y la aceptación de la gestión de la calidad, y la mejorará cuando sea necesario; comunicará de manera eficaz el enfoque.

APO09.02 Definir estándares, procesos y prácticas de calidad. – Identificará requisitos, normas, procedimientos y prácticas de los procesos clave para orientar a la entidad en el cumplimiento del SGC.

Hará uso de las mejores prácticas existentes como referencia para la mejora y adaptación de los procesos de gestión de la calidad; y considerará los costos y beneficios de las certificaciones de calidad.

APO09.03 Supervisar y hacer controles y revisiones de calidad. – Definirá, planificará y supervisará la calidad de los procesos y servicios de forma permanente como se defina en el SGC, con medidas para medir la satisfacción del cliente con la calidad, así como el valor que proporciona el SGC.

Supervisará la calidad de los procesos y servicios de forma permanente y sistemática mediante la descripción, métricas, análisis, ingeniería y controles de los procesos; llevará a cabo revisiones de calidad e informará los resultados de las revisiones y pondrá en marcha las mejoras necesarias.

APO09.04 Integrar la gestión de la calidad en la implementación de soluciones, entrega de servicios y mejora continua. – Incorporará las prácticas pertinentes de gestión de la calidad en el desarrollo de soluciones y prestación de servicios ofrecidos; y promoverá una cultura de calidad y mejora continua.

Analizará datos sobre el SGC y definirá periódicamente un plan de la calidad que promueva la mejora continua; identificará casos recurrentes de no conformidades, defectos de calidad, determinará su causa raíz, evaluará su impacto y aplicará acciones de mejora de manera oportuna para permitir que se adopten las medidas correctivas.

3.2.10 APO10 Administrar el riesgo

La unidad de Tecnología de la Información administrará identificar, evaluará y reducirá los riesgos relacionados con TI de forma continua.

APO10.01 Recopilar datos. – Identificará y recopilará datos relevantes para una identificación, análisis y notificación efectiva de riesgos relacionados con TI.

Establecerá un método para la toma, clasificación y análisis de datos relacionados con riesgo de TI, analizará datos históricos de los mismos y de pérdidas experimentadas tomados de datos y tendencias externas disponibles; ejecutará análisis periódicos de eventos y de factores de riesgo identificar asuntos emergentes relacionados con el riesgo.

APO10.02 Analizar el riesgo. – Desarrollará información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la criticidad para el negocio.

Diseñará escenarios de riesgo de TI, estimará la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI; tendrá en cuenta todos los factores de riesgo que apliquen, evaluará controles operacionales conocidos y estimará niveles de riesgo residual, validará los resultados de análisis de riesgos para la toma de decisiones, confirmando que los análisis se alinean con requerimientos de la entidad.

APO10.03 Mantener un perfil de riesgo. – Desarrollará un inventario del riesgo conocido, atributos de riesgo y de otros recursos, capacidades y actividades de control actuales relacionados.

Realizará el inventario los procesos de negocio, incluirá el personal de soporte, aplicaciones, infraestructura, instalaciones, manuales críticos y documentará la dependencia; determinará y acordará servicios y recursos de infraestructuras de tecnología esenciales para sostener las operaciones, registrará información sobre eventos de riesgos de TI que se han materializado, para su inclusión en el perfil de riesgo tecnológico de la entidad.

APO10.04 Expresar el riesgo. –Proporcionará información sobre el estado actual de exposiciones y oportunidades relacionadas con TI a las partes interesadas y necesarias para una respuesta apropiada.

Informará los resultados del análisis de riesgos a todas las partes afectadas en términos y formatos útiles para un entendimiento de los escenarios y que permita la toma de decisiones por parte de los responsables de la entidad.

APO10.05 Definir acciones para control y respuesta al riesgo. –Identificará las oportunidades para reducir el riesgo a un nivel aceptable; y responderá de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.

Mantendrá un control de cambios de las actividades de contingencia que estén en marcha para mitigar el riesgo de TI, escenarios de contingencia, definirá un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo en TI, contemplará el uso de un centro de cómputo alterno de uso compartido en un Centro de Datos del Estado, mientras dure la contingencia; preparará planes que detallen los pasos específicos (previos, durante y después) a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente grave con un impacto al negocio, designará un comité con roles específicos y nombre de los encargados de ejecutar las actividades de contingencia y aplicará el plan de respuesta apropiado (plan de contingencia) para minimizar el impacto.

3.2.11 APO11 Administrar la seguridad

La unidad de Tecnología de la Información definirá, operará y supervisará un sistema para la gestión de la seguridad de la información (confidencialidad, disponibilidad, integridad).

APO11.01 Constituir y conservar un SGSI. – Implantará un SGSI que facilite un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y

procesos de negocio que se encuentren alineados a los requerimientos y la gestión de seguridad de la entidad.

Definirá un SGSI de acuerdo con la política de entidad; mantendrá contacto con personal especializado en temas relacionados con seguridades, especificará el alcance y los límites del SGSI en términos de las características de la entidad, la organización, su localización, activos y tecnología. Incluirá una justificación para, cualquier exclusión del alcance, obtendrá el permiso de las autoridades correspondientes para implementar y ejecutar o cambiar el SGSI; definirá y comunicará los roles y las responsabilidades de la gestión de la seguridad de la información.

APO11.02 Definir y operar un plan de tratamiento del riesgo de la seguridad de la información. – Mantendrá un plan de seguridad de información que describa cómo se administran y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de entidad. Supervisará que las recomendaciones de mejoras en seguridad se basan en casos de negocio aprobados, y que se implementan como parte integral del desarrollo de soluciones.

Desarrollará propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que consideren la financiación, asignación de roles y responsabilidades y control de accesos no permitidos al código fuente de las aplicaciones; recomendará programas de formación sobre seguridad de la información; e integrará controles de seguridad de la información que permitan prevenir y detectar con anticipación eventos de seguridad, y la respuesta ante incidentes.

APO11.03 Supervisar y revisar el SGSI. – Analizará datos sobre el SGSI e informará periódicamente sobre la necesidad y los beneficios de la mejora continua en lo referente a seguridad de información e impulsará una cultura de seguridad y de mejora continua.

Realizará revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerará los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas, para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.

3.3 Construcción, Adquisición e Implementación (CAI)

Este dominio contiene 10 procesos encargados de diseñar e implementar las soluciones identificadas en el dominio APO, convirtiéndolas en servicios a la entidad.

3.3.1 CAI01 Administrar Programas y Proyectos

La unidad de Tecnología de la Información administrará (iniciará, planificará, controlará y ejecutará) todos los programas y proyectos que formen parte del plan anual de inversiones de la unidad de TI, de forma coordinada y alineadas con la estrategia corporativa; y supervisará el cierre de los mismos con una revisión post-implementación.

CAI01.01 Mantendrá la estandarización en los programas y proyectos. - Mantendrá la estandarización sobre los programas y los proyectos informáticos para ejecutar tomar decisiones de gobierno orientadas a conseguir valor (requisitos, riesgos, costes, cronograma y calidad).

Administrará los programas y proyectos (inicio, planeación, ejecución, control, monitoreo y cierre de proyectos), alineado con los objetivos de la entidad, a las buenas prácticas y al uso de tecnología adecuada; esta administración incluirá objetivos, alcance, recursos, riesgos, costo total (costos directos, indirectos), calidad, cronograma de actividades, comunicaciones, entregables, aprobaciones, compromisos de las partes interesadas, adquisiciones, control de

cambios, integración, generación de beneficios y bitácora de lecciones aprendidas, mediante el uso de actas o documentos.

CAI01.02 Iniciar, desarrollar, mantener, lanzar y ejecutar un programa. – Iniciará un programa con el objetivo de evidenciar las metas alcanzadas, incluyendo el patrocinio del programa, designación de los consejeros del programa, generación de la documentación, actualización del caso de negocio, desarrollo de un plan de beneficios y alcance de la aprobación de los interesados; formulará un programa con el objetivo de definir las bases y formalizará el alcance de trabajo identificando los entregables que cumplirán con los objetivos planteados; mantendrá actualizado el plan y asegurará el cumplimiento de los objetivos estratégicos mediante este programa; y liberará el programa para adquirir los recursos necesarios para conseguir los objetivos del programa; preparará los cambios de fase y las revisiones; y establecerá los fundamentos para financiar las etapas posteriores.

CAI01.03 Administrar el compromiso de los interesados. – Conducirá el compromiso de los interesados en obtener información oportuna, consistente y precisa.

Planificará la forma de identificar a las partes interesadas y que se encontrarán inmersas en el ciclo de vida de los proyectos; comprometerá a los interesados manteniendo la coordinación y comunicación adecuada; medirá la efectividad del compromiso que tienen las partes; y analizará los intereses y requisitos de las partes interesadas.

CAI01.04 Revisar, controlar y comunicar los resultados del programa. – Vigilará el rendimiento del programa e informará los resultados al comité estratégico del programa.

Controlará los recursos y activos de TI que han sido modificados durante el programa; identificará las desviaciones del programa y tomará las acciones necesarias para su corrección;

actualizará el portafolio de servicios conforme los cambios que sufran; y revisará los criterios de cambio de fase para la toma de decisiones.

CAI01.05 Lanzar e iniciar proyectos dentro de un programa. – Documentará el alcance del proyecto y la forma en que se relaciona con otros proyectos; y contará con la aprobación del patrocinador del proyecto.

Creará un entendimiento común del proyecto para las partes interesadas; asegurará que cada proyecto tenga un patrocinador con autoridad suficiente para la ejecución del mismo; asegurará que los patrocinadores y los interesados del proyecto estén de acuerdo en los requerimientos; se cerciorará de que la definición del proyecto cubre los requerimientos de las partes interesadas; y realizará el seguimiento de la ejecución de cada proyecto.

CAI01.06 Planificar proyectos. – Establecerá un plan de proyectos integrado y aprobado para controlarlo durante todo el ciclo de vida, el alcance deberá estar definido para aumentar la capacidad de la entidad.

Desarrollará un plan de proyectos que incluya los entregables, criterios de aceptación, recursos y responsabilidades; asegurará una comunicación efectiva y que los planes efectuados se reflejan en otros proyectos; determinará las actividades que se realizarán en el proyecto; verificará que cada hito contiene un entregable; y establecerá una base para el proyecto.

CAI01.07 Administrar la calidad de los programas y proyectos. – Ejecutará un plan sobre el aseguramiento de la calidad que esté alineado al Sistema de Aseguramiento de la Calidad, el que deberá estar aprobado por las partes interesadas; para ser incluido en los planes de los programas.

Identificará las actividades importantes sobre aseguramiento para garantizar los sistemas nuevos o modificados; entregará garantías de calidad sobre los productos; y realizará aseguramiento de la calidad del proyecto.

CAI01.08 Administrar el riesgo de los programas y proyectos. – Minimizará los riesgos relacionados al proyecto a través de la supervisión de los eventos y sus causas.

Definirá un enfoque de gestión de riesgos sobre el proyecto y definirá los responsables de su ejecución; ejecutará un análisis de riesgos para cuantificar los mismos y los evaluará de forma continua; y registrará los posibles eventos que puedan suscitarse.

CAI01.09 Supervisar y controlar proyectos. – Medirá el desempeño del proyecto contra la planificación, los costos, riesgos y la calidad; y evaluará el impacto de sufrir desviaciones.

Definirá criterios para el proyecto y medirá el rendimiento con base en los mismos; comunicará sobre el avance del proyecto; supervisará los cambios y los documentará; obtendrá la aprobación de los entregables de cada fase usando criterios definidos de aceptación; y mantendrá un sistema de control de cambios para el proyecto.

CAI01.10 Administrar los recursos y los paquetes de trabajo del proyecto. – Administrará los trabajos de TI a través de requerimientos formales, a los que se les asignarán los paquetes de trabajo.

Identificará los recursos necesarios para el proyecto incluyendo las habilidades y el tiempo necesario, así como un líder de proyecto con la experiencia suficiente; definirá los roles de todos los involucrados; incluirá seguridad de la información dentro del proyecto, autorizará la ejecución del plan de proyecto; identificará las diferencias entre la planificación y la realización del programa.

CAI01.11 Cerrar un proyecto o iteración y el programa. – Coordinará la entrega de los productos y la culminación de hitos con los interesados del proyecto; identificará actividades pendientes y lecciones aprendidas de la fase o el proyecto; y eliminará el proyecto del portafolio de TI una vez que se haya culminado exitosamente el mismo.

Definirá los pasos claves para culminar el proyecto; revisará de forma posterior la implementación; y obtendrá la aceptación de los entregables.

3.3.2 CAI02 Administrar la definición de requisitos

La unidad de Tecnologías de la Información y Comunicaciones identificará soluciones y requerimientos que estén alineados con los objetivos de la entidad; y coordinará con las partes interesadas la viabilidad de realizar proyectos de TI para solventar las necesidades de la institución.

CAI02.01 Definir requerimientos técnicos y funcionales de negocio. – Identificará los requerimientos del negocio, funcionales, técnicos y de control para alcanzar las metas propuestas por TI.

Establecerá un repositorio de requerimientos funcionales y técnicos; priorizará la información referente a los requisitos; validará la aceptación de los aspectos claves; controlará el alcance de los requerimientos; y considerará todos los tipos de requisitos que incluyan estándares, políticas empresariales, temas de seguridad, tecnologías, etc.

CAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas. – Analizará la viabilidad de las soluciones posibles y considerará la posibilidad de realizar un piloto para determinar posibles mejoras.

Identificará los requisitos necesarios para la adquisición de la solución; revisará las posibles soluciones con las partes interesadas; y definirá los recursos y las fases necesarias para la implementación.

CAI02.03 Administrar los riesgos de las necesidades. – Identificará y clasificará los riesgos funcionales y técnicos que tengan relación con el análisis de la información relacionada con las necesidades de la solución propuesta para la institución.

Creará una lista que incluya los requerimientos técnicos y funcionales relacionados al análisis de los datos; analizará los riesgos a los que están expuestos los requerimientos según la probabilidad y el impacto que pudieran presentarse; e identificará formas de mitigarlos o controlarlos.

CAI02.04 Obtener la aprobación de los requerimientos y soluciones. – Mantendrá una retroalimentación con las partes interesadas y obtendrá la aprobación para el cierre de requerimientos y soluciones recomendadas.

Asegurará que la decisión final sobre la elección de la solución es tomada por el patrocinador (dueño del negocio) y mantendrá revisiones de calidad de todas las fases del proyecto para la firma del patrocinador.

3.3.3 CAI03 Administrar la identificación y construcción de soluciones

La Dirección de Tecnologías de la Información establecerá soluciones alineadas a los requerimientos de la entidad; además coordinará la realización de pruebas, configuraciones y el mantenimiento de los procesos relacionados.

CAI03.01 Diseñar soluciones de alto nivel. – Documentará soluciones de alto nivel mediante desarrollo ágil; mantendrá la arquitectura empresarial y los diseños actualizados; principios de sistemas de seguridad y se asegurará de que los interesados tengan una participación constante.

Traducirá la solución de alto nivel en los requerimientos de la entidad manteniendo involucradas a las partes interesadas; creará un diseño con adopción y aplicación de políticas públicas y estándares internacionales para: el código y nomenclaturas del lenguaje de programación, interfaces de usuario, interoperabilidad, tiempo de respuesta de los sistemas, escalabilidad; y presentará el diseño final su aprobación.

CAI03.02 Diseñar los componentes detallados de la solución. – Usará técnicas de desarrollo ágil para la elaboración de los diseños y manuales incluyendo OLAs y SLAs internos y externos.

Diseñará las actividades, procesos, diseños físicos y lógicos, transacciones, reglas de negocio, controles de aplicación y de base de datos, tipos de datos, interfaces, clasificará las entradas y salidas de datos conforme la arquitectura empresarial; diseñará las interfaces, el almacenamiento, pistas de auditoría y la redundancia; considerará el impacto del sistema tomando en cuenta la infraestructura que posee; y definirá métodos para evaluar las transacciones, manuales técnicos, de usuario y problemas generados.

CAI03.03 Desarrollar los componentes detallados de la solución. – Desarrollará de manera progresiva los componentes del sistema manteniendo los estándares y asegurará que mantengan controles de seguridad sobre las aplicaciones, bases de datos y servicios de TI.

Definirá el soporte y mantenimientos tantos internos como de proveedores en caso de ser externo; documentará los componentes y cambios de la solución; evaluará el impacto de las parametrizaciones que se realizarán; y definirá claramente las responsabilidades para usar las seguridades apropiadas en el ambiente de desarrollo aislado tanto del ambiente de pruebas como de producción.

CAI03.04 Obtener los componentes de la solución. – Conseguirá que los componentes de la solución se establezcan conforme lo definido en los requisitos con calidad y estándares; y que en caso de proveedores cumplan con todos los términos contractuales.

Creará y revisará un plan de adquisiciones aprobado por la máxima autoridad para la solución y los ítems relacionados a ella; considerará el incremento de capacidades; y documentará los beneficios adicionales que se pueden presentar.

En la adquisición de hardware, los contratos tendrán el detalle suficiente de las características técnicas de los componentes tales como: marca, modelo, número de serie, capacidades, entre otros, y las garantías solicitadas al proveedor, a fin de establecer la correspondencia entre los equipos adquiridos y las especificaciones técnicas establecidas

CAI03.05 Construir soluciones. – Configurará las soluciones para integrarlas en los procesos de la entidad en software y hardware; incluirá controles de seguridad y de auditoría; y actualizará el catálogo de servicios de TI.

Considerará la información relevante en la implementación de los controles y las pistas de auditoría; validará la interoperabilidad de la solución y el cumplimiento de requerimientos; y establecerá el derecho de propiedad intelectual sobre el software adquirido con código fuente.

CAI03.06 Realizar controles de calidad. – Ejecutará un plan de calidad para verificar que la solución cumple con los requisitos de calidad solicitados conforme las políticas de la entidad.

Supervisará de forma continua la calidad de la solución realizando pruebas de código, automáticas e integrales; y conservará un registro de todas las revisiones con sus respectivos resultados.

CAI03.07 Preparar y ejecutar pruebas para la solución. – Desarrollará y ejecutará un plan de pruebas para los componentes de forma individual e integral, incluyendo la

infraestructura sobre la que se encuentra implementada, y que cumpla con las estrategias de la entidad.

Ejecutará el plan de pruebas desarrollado usando instrucciones definidas de forma clara; usará información real y la mantendrá con las seguridades correspondientes; verificará que se realicen de forma integral; e identificará, clasificará y registrará los errores y los resultados de las mismas.

CAI03.08 Administrar cambios en los requerimientos. – Realizará el seguimiento sobre los requerimientos durante todo el ciclo de vida del proyecto; evaluará el impacto de los cambios solicitados; y aplicará las solicitudes de cambio verificando que se mantenga la integridad e integración de la nueva solución.

CAI03.09 Mantener soluciones. – Definirá un plan de mantenimiento para las soluciones y componentes de la infraestructura, donde incluya requerimientos periódicamente; supervisará que se aplique el proceso de desarrollo en caso de existir cambios mayores que deban realizarse; buscará tendencias anormales para definir si existen problemas de rendimiento; y vigilara la usabilidad del proceso de cambios.

CAI03.10 Delimitar los servicios TI y conservar el catálogo de servicios. – Establecerá servicios nuevos de tecnología y comunicaciones y los documentará, incluyendo cambios y niveles de servicio que serán considerados en el portafolio y coordinará su aprobación por la autoridad competente.

3.3.4 CAI04 Administrar la disponibilidad y la capacidad

La Dirección de TI evaluará las capacidades con las que cuenta actualmente la entidad para abastecer las necesidades de capacidad, rendimiento y disponibilidad conforme los requisitos existentes.

CAI04.01 Calcular la disponibilidad, rendimiento y capacidad existente y establecer una línea base. – Soportará los requisitos de la institución mediante la evaluación de capacidad y rendimiento de los recursos y servicios para cumplir con los niveles de operación acordados.

Controlará la capacidad y rendimiento evaluando los resultados reales contra los umbrales definidos; identificará los incidentes presentados por rendimiento o capacidad; y comparará las tendencias presentadas con los SLAs tomando en cuenta las variables del entorno.

CAI04.02 Evaluar el impacto en el negocio. – Determinará los servicios críticos para los procesos del negocio con el fin de mantener el cumplimiento de los SLAs; creará escenarios con la capacidad existente para evaluar la disponibilidad y probar su cumplimiento; explicará el impacto obtenido con las pruebas realizadas; y comunicará los resultados de las pruebas.

CAI04.03 Planificar requisitos de servicios nuevos o modificados. – Priorizará los cambios de las necesidades de la entidad en lo referente a capacidad, disponibilidad y rendimiento validando las implicaciones; creará planes de capacidad y disponibilidad tomando como base los procesos de negocio.

CAI04.04 R**evisar la capacidad y disponibilidad. –** Revisará, analizará y comunicará sobre la capacidad, disponibilidad y rendimiento a través de la recolección de datos; y proveerá informes para gestionar el presupuesto de la unidad.

CAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad. – Investigará sobre los incidentes reportados sobre capacidad y rendimiento mediante la guía de manuales; identificará las brechas presentadas en el rendimiento y la capacidad; definirá acciones correctivas y un procedimiento de escalado cuando se presenten emergencias.

3.3.5 CAI05 Administrar cambios organizativos

La Dirección de Tecnologías de la Información y Comunicaciones cubrirá todo el ciclo de vida de los cambios y las partes interesadas para asegurar una implementación exitosa.

CAI05.01 Establecer el deseo de cambiar. – Entenderá el impacto que provoca el cambio y la disposición por parte de los interesados; identificará las acciones que deben realizarse para tener un cambio exitoso; encontrará los puntos de conflicto al realizar un cambio; y motivará a las partes interesadas a involucrarse en el cambio.

CAI05.02 Formar un equipo de implementación efectiva y comunicar la visión deseada. – Establecerá un equipo con las personas correctas que tengan metas en común y medidas efectivas alineadas a los objetivos de la entidad.

Comunicará de una forma entendible la visión, el impacto, los beneficios y los responsables del cambio; reforzará la comunicación y verificará el nivel de entendimiento alcanzado.

CAI05.03 Facultar a los que juegan rol, identificar ganancias en el corto plazo y facilitar la operación y el uso. – Asignará responsabilidades y alineará la estructura organizativa con ayuda de Talento Humano; comunicará las ganancias que se puedan obtener en el corto plazo aplicando el cambio; y planificará la necesidad de capacitar al personal relacionado.

Implementará lo necesario en el aspecto tecnológico y de operación para que el personal pueda desarrollar sus funciones; definirá métricas para medir la satisfacción del personal con los cambios implementados.

CAI05.04 Integrar nuevos enfoques. – Integrará nuevos puntos de vista después de dar seguimiento al cambio implementado e identificará la efectividad que tuvo el plan de mantenimiento y comunicación; verificará que los responsables ejecuten los procesos día a día.

CAI05.05 Mantener los cambios. – Transferirá los conocimientos y capacitará al personal; mantendrá comunicados a los interesados sobre los cambios y el compromiso de las autoridades para mantenerlos; mantendrá una base de conocimiento sobre las lecciones aprendidas y las socializará.

3.3.6 CAI06 Administrar los cambios

El área de Tecnologías de la Información administrará los cambios manteniendo un control, aplicando procedimientos, documentación, análisis de impacto, priorización, etc.

CAI06.01 Evaluar, priorizar y autorizar peticiones de cambio. – Entenderá el impacto que provoca el cambio y analizará si es negativo; creará peticiones formales para solicitar cambios y los categorizará y priorizará tanto de forma interna como los realizados por los proveedores; aprobará formalmente cada uno de los cambios solicitados; y evaluará los servicios contratados con respecto a los cambios.

CAI06.02 Administrar cambios de emergencia. – Tendrá cuidado con los cambios emergentes para evitar futuros incidentes y los aprobará; desarrollará un procedimiento para el tratamiento de cambios de emergencia; validará que los accesos para ejecutar los cambios emergentes han sido aprobados; revisará de forma posterior la implementación de los cambios; y definirá qué y cuáles son los cambios emergentes.

Mantendrá un sistema de seguimiento sobre los cambios rechazados, aprobados y cerrados; categorizará los cambios y elaborará informes sobre el rendimiento de los mismo; documentará las actualizaciones que se realicen sobre los cambios implementados y definirá un tiempo máximo de conservación de esta información y la revisará periódicamente.

3.3.7 CAI07 Administrar la aceptación del cambio y la evolución

El área de Tecnologías de la Información formalizará la operatividad de las nuevas soluciones, con su implementación, la transformación de los datos, las pruebas y la comunicación, el paso a producción y el soporte.

CAI07.01 Definir un plan de implementación. – Desarrollará un plan que incluya la implementación del sistema, la transformación de los datos, las pruebas de aceptación, la comunicación, el soporte y al plan de retorno al estado anterior.

Confirmará que las partes interesadas aprobaron el plan y que los proveedores participarán en cada paso de la implementación; mantendrá vigente el proceso de retorno al estado anterior y analizará los riesgos que son parte del proceso.

CAI07.02 Planear la transformación de procesos de la entidad, sistemas e información. – Migrará los procesos, la información y los servicios de la entidad, así como la infraestructura de TI como parte de la innovación de la misma; definirá los roles de los responsables de este proceso y métodos para validar la migración correcta de los datos; validará de forma previa el proceso de migración; y planificará la generación de pistas de auditoría y almacenamiento de los respaldos correspondientes para cumplir con la normativa.

CAI07.03 Planear y ejecutar pruebas de aceptación. – Definirá un plan de pruebas que cuente con los roles y responsabilidades, definiciones de entrada y salida; y verificará su aprobación, el plan de pruebas incluirá los recursos necesarios para su ejecución, además de la identificación de los riesgos del proyecto; y tomará en cuenta las fases adecuadas para su implantación.

Revisará los criterios de evaluación y aceptación de las pruebas ejecutadas en contraste con las definidas en el plan; formalizará la aceptación de las pruebas a través de la firma de terceros; realizará pruebas de seguridad conforme el plan que incluirá al menos las aplicaciones críticas e identificará y clasificará los errores observados en las pruebas para realizar correcciones y mejoras en la calidad.

CAI07.04 Definir un ambiente de pruebas. – Establecerá un ambiente de pruebas independiente de forma física y lógica que represente al ambiente de producción de la entidad que comprenda la capacidad, rendimiento, controles, calidad de la información y la seguridad necesaria.

Mantendrá una base de datos con información real pero representativa, que se encuentre segura; asegurará el perímetro del ambiente de pruebas con el fin de que no tenga acceso al de producción.

CAI07.05 Pasar a producción y controlar la implementación de versiones. – Pondrá en producción la solución aceptada mediante proyectos piloto o de forma paralela a la solución anterior hasta probar su correcto funcionamiento; administrará mediante procedimientos definidos la liberación de los diferentes componentes; actualizará la documentación del sistema(procedimientos, procesos, manuales); notificará a los usuarios e interesados sobre la implementación; y mantendrá un control y registro (versionamiento) de las implementaciones automáticas o manuales que se realicen.

CAI07.06 Brindar soporte y realizar una revisión posterior en el ambiente de producción. – Brindará soporte a todos los usuarios e interesados desde el primer momento para evitar incidencias durante un tiempo determinado.

Ejecutará una evaluación posterior a la implementación para verificar los resultados y los comparará con los esperados; consultará a los interesados sobre posibles métricas usables para evaluar el desempeño de la implementación; tomará en cuenta lo definido en el proceso de gestión de cambios para realizar la evaluación de niveles de servicio y operación; e implementará acciones en caso de encontrarse incidentes en la revisión.

3.3.8 CAI08 Administrar el conocimiento

La Dirección de TI conservará el conocimiento importante, validado y confiable para dar soporte a las actividades, facilitando la toma de decisiones; lo clasificará y organizará para su uso.

CAI08.01 Cultivar una cultura de traspaso de conocimientos. – Implementará un esquema para facilitar el intercambio de conocimientos a través de motivaciones, herramientas y el entorno propicio.

CAI08.02 Clasificar y organizar las fuentes de información y transformarlas en conocimiento. – Clasificará las fuentes internas y externas de información para facilitar el uso de los procesos de la entidad y los servicios tecnológicos. Identificará a los usuarios y propietarios de la información que puede ser compartida, así como el contenido de la misma; y validará las fuentes de información antes de ponerla en conocimiento de los demás.

Organizará la información relacionándola, definiendo niveles de acceso y creando vistas para los usuarios interesados.

CAI08.03 Utilizar, compartir, evaluar y retirar la información. – Difundirá las fuentes de información entre los interesados y explicará las herramientas que pueden usar para aprovechar estos recursos según las necesidades.

Medirá la importancia y el uso dado a la información; e identificar el conocimiento que ya no es relevante o es inútil y definirá reglas para eliminarlo.

3.3.9 CAI09 Administrar los activos

La unidad de tecnología administrará los activos de TI con el objetivo de asegurar que el uso de éstos mantiene un valor y están justificados para apoyar en los servicios tecnológicos; administrará las licencias de software para verificar que la cantidad adquirida es la requerida, que cumple con los acuerdos de licencia.

CAI09.01 Registrar los activos. – Conservará un registro de los activos de TI con los que presta servicios y garantiza su alineación de configuración y finanzas; el registró contendrá el estado y todos los requisitos que se encuentran en el Reglamento de Bienes del Sector Público, contemplará la devolución de los activos cuando un funcionario o servidor público cese de sus

funciones; realizará tomas de inventario de bienes informáticos, con el detalle de las características y responsables a cargo, conciliado con los registros contables de forma permanente para definir el período de vida útil y ejecutará la contabilización de los mismos.

CAI09.02 Administrar activos críticos. – Identificará los activos críticos en la prestación de servicios tecnológicos y los mantendrá disponibles; verificará el rendimiento de los activos examinando las incidencias y considerando los riesgos existentes; ejecutará mantenimientos preventivos a todos los activos especialmente a los críticos, contando con personal calificado y validando el factor costo-beneficio; mantendrá informados a los interesados cuando se realicen mantenimientos; planificará ventanas de mantenimiento para minimizar el impacto; y asegurará que los accesos remotos estén activos únicamente el tiempo necesario.

CAI09.03 Administrar el ciclo de vida de los activos. – Administrará los activos desde su compra hasta su dada de baja con el fin de asegurar el uso eficiente y eficaz de los mismos; adquirirá activos únicamente mediante solicitudes aprobadas y cumpliendo con las políticas de la entidad; registrará los activos y completará el proceso de adquisición; distribuirá los activos a los custodios responsables; reasignará los activos cuando se encuentren sin uso y en buenas condiciones; asegurará de forma previa a la re asignación de los activos de que éstos no contienen información sensible o crítica; y dará de baja los activos de forma segura, incluyendo dispositivos móviles, y cumpliendo con la normativa.

CAI09.04 Mejorar el valor de los activos. – Validar constantemente el inventario general de activos con el fin de mejorar los costos y mantener satisfechas las necesidades institucionales.

Revisará las garantías de los activos; identificará activos subutilizados y sobre utilizados para mantenerlos en un uso normal; y revisará el estado de los mismos para aprovechar tecnologías alternativas que reduzcan costos.

CAI09.05 Administrar licencias. – Administrará las licencias con el fin de mantener el número adecuado para satisfacer las necesidades de la entidad; mantendrá un inventario de las licencias existentes; validará el número de copias de software instalado y verificará si son necesarias para los usuarios, caso contrario buscará tomará acciones para mejorar los costos y el número de licencias.

3.3.9 CAI10 Administrar la configuración

La Dirección de Tecnologías de la Información definirá los recursos principales para la prestación de servicios, incluyendo las configuraciones con sus pistas de auditoría y la actualización del repositorio de información.

CAI10.01 Definir un estándar de configuraciones. – Establecerá un modelo de la infraestructura, servicios activos y las configuraciones de los mismos; definirá el alcance y los niveles de configuración; y definirá un modelo que incluya lo necesario para mantener una configuración adecuada en la entidad.

CAI10.02 Definir un repositorio de configuraciones con una línea base y actualizarlo. – Mantendrá un repositorio de configuraciones y creará líneas base sobre configuraciones controladas; clasificará las configuraciones y las almacenará; y documentará y formalizará un acuerdo sobre las líneas base de las configuraciones.

Mantendrá actualizado el repositorio identificando los cambios realizados; garantizará la integridad y precisión de las configuraciones a través de la actualización de las líneas base.

CAI10.03 Elaborar informes de estado y configuración. – Elaborará informes sobre los cambios realizados en las configuraciones; identificará cambios no autorizados; e identificará las necesidades de los interesados.

CAI10.04 Validar la integridad del repositorio de configuraciones. – Evaluará periódicamente el repositorio de configuraciones para asegurar la integridad; comparará las

configuraciones tanto físicas como lógicas y comunicará sobre cualquier novedad encontrada; revisará que la base de configuraciones se encuentre completa y precisa.

3.4 Entrega, Servicio y Soporte (ESS)

Este dominio está formado por 6 procesos relacionados con la entrega de servicios de TI, que cumplen con el objetivo de entregar servicios alineados a las prioridades de la entidad, mediante la implementación de la confidencialidad, la integridad y la disponibilidad de forma correcta.

3.4.1 ESS01 Administrar Operaciones

La unidad de Tecnología de la Información coordinará y pondrá en marcha los procedimientos operativos necesarios para una entrega de los servicios tecnológicos tanto internos como externos, de acuerdo a lo planificado y tomando en cuenta las actividades de monitoreo, así como los procedimientos operativos estándar.

ESS01.01 Ejecutar procedimientos operativos. – Documentará y ejecutará procedimientos y tareas operativas que sean confiables y consistentes como, por ejemplo: planes de uso y operación de los equipos de respaldos, guías de implementación de seguridad de la información en la arquitectura de los servicios tecnológicos, instalación segura de software, etc.

Desarrollará procedimientos y actividades operativas con el objetivo de apoyar a todos los servicios tecnológicos entregados, mismos que servirán para gestionar el desempeño y el rendimiento de las tareas programadas; asegurará que se cumplen con los estándares necesarios para la recepción, procesamiento, almacenamiento y salida de información, cumpliendo con la política de seguridad y satisfaciendo los objetivos de la entidad. Ejecutará y registrará las copias de respaldos de la información conforme los procedimientos establecidos por la entidad; y sincronizará los relojes de todos los sistemas de procesamiento.

ESS01.02 Administrar los servicios externos de TI. - Administrará los servicios externos que mantiene la entidad con el fin de precautelar la integridad y confidencialidad de la información y los activos tecnológicos en la entrega de los servicios a través de Acuerdos de Nivel de Operaciones y Acuerdos de Nivel de Servicios.

Asegurará que los contratos y los acuerdos de nivel de servicios (SLAs) con terceros, cumplan con los requerimientos de seguridad de la entidad; procurará que se integren los servicios críticos de la entidad con los proveídos por terceros (gestión de la configuración, de cambios, de incidentes, de seguridad, capacidad de rendimiento, etc.); y planificará auditorías de los servicios externos con el fin de validar que estos servicios se estén brindado de una forma adecuada.

ESS01.03 Supervisar la infraestructura de TI. - Supervisará la infraestructura tecnológica y almacenará la información sobre los incidentes de la misma para realizar reconstrucciones o revisiones en caso de ser necesario.

Mantendrá un monitoreo continuo sobre los activos de infraestructura que proveen servicios catalogados como críticos y realizará un inventario de los mismos, registrará mediante la creación de tickets los eventos significativos que registren violaciones de umbral y los almacenará durante un tiempo no menor a 7 años para efectuar revisiones posteriores con los proveedores de servicios o equipos de la infraestructura de la entidad.

ESS01.04 Administrar el entorno. - Proveerá de los recursos necesarios para proteger los activos y la información de factores ambientales, por ejemplo: extintores dentro del centro de datos, detectores de temperatura, humo y de humedad, etc.

Identificará los posibles desastres naturales que puedan presentarse y afectarán los recursos y activos de tecnología, así como el impacto que causarían en la entidad; verificará las

protecciones con las que cuenta la institución para equipos internos y externos; además, validará que la política de seguridad incluya la prohibición de ingerir alimentos, bebidas y cigarrillos en áreas sensibles; mitigará los riesgos a los que se encuentran expuestas las instalaciones de TI; mantendrá un monitoreo continuo sobre los dispositivos que detectan proactivamente las amenazas del entorno; documentará y evaluará los procedimientos de respuesta a incidentes incluyendo los contactos importantes para atender los mismos; comparará los planes de contingencia que forman parte de las pólizas de seguro; se cerciorará de que los lugares donde se encuentren las instalaciones de TI cuenten con un diseño y construcción apropiada para mitigar los riesgos naturales; y mantendrá las salas de tecnologías de la información limpias y en buenas condiciones.

ESS01.05 Administrar las instalaciones. - Tramitará que todas las instalaciones de TI cumplan con las regulaciones de la entidad, directrices de salud y seguridad del trabajo, como son las instalaciones eléctricas acondicionadas y las de comunicaciones con las que cuenta la entidad.

En caso de ser requerido dispondrá de sistemas de alimentación eléctrica que permitan mantener la energía en caso de interrupciones del fluido eléctrico (baterías, generadores, UPS, etc.) y realizará pruebas para verificar el funcionamiento correcto de dichos equipos; validará que el cableado externo cuente con una protección adecuada y se encuentre bajo tierra y únicamente personas con autorización tengan acceso al mismo; contará con redundancia y tolerancia a fallos sobre el cableado y lo mantendrá organizado; capacitará al personal sobre los incidentes que podrían sufrir y las acciones que deberían realizar en caso de una eventualidad; se asegurará de que los mantenimientos sean realizados únicamente por personal autorizado; y analizará el riesgo al que se encuentra expuesto el entorno de TI mediante las alteraciones físicas reportadas.

3.4.2 ESS02 Administrar Peticiones e Incidentes de Servicio

Brindará una respuesta oportuna a los incidentes reportados por los usuarios, recuperando los servicios y poniéndolos operativos; así como registrando, reportando y escalando los incidentes.

ESS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio. - Desarrollará esquemas de incidentes y los clasificará a través de Acuerdos de Nivel de Servicios, esquemas de clasificación de problemas, entre otros.

Realizará una priorización de los incidentes y las peticiones de servicio de los usuarios y los mantendrá informados sobre las soluciones; definirá modelos sobre las incidencias reportadas para crear una base de conocimientos y prestar soluciones de una forma eficaz; y detallará procedimientos para escalar los incidentes.

ESS02.02 Registrar, clasificar y priorizar peticiones e incidentes. - Identificará, registrará y clasificará los incidentes, los priorizará según su criticidad y lo definido en los acuerdos de nivel operativo y de servicio establecidos.

Registrará todos los casos reportados por los usuarios manteniendo la información relevante para ser administrada y usada de forma efectiva; definirá un tipo y una categoría para los eventos registrados; y clasificará los incidentes según lo establecido en los OLAs y SLAs.

ESS02.03 Verificar, aprobar y resolver peticiones de servicio. - Seleccionará la solución apropiada para los requerimientos y validará de forma previa que el mismo cumpla con los parámetros definidos para la solicitud.

Establecerá un flujo de proceso para la solicitud de servicio; realizará los cambios necesarios una vez que cuente con la autorización funcional o documental; y facilitará las

peticiones de los usuarios a través de programas informáticos que cuenten con menús automáticos y los requerimientos frecuentes.

ESS02.04 Investigar, diagnosticar y localizar incidentes. - Identificará posibles incidentes relacionados con TI dentro de la entidad, determinará las posibles causas que los ocasionan y buscará soluciones a los mismos.

Determinará los síntomas de los eventos y los motivos por los que suceden para buscar posibles soluciones; registrará los problemas nuevos que se presenten y asignará los incidentes a los especialistas de la unidad de TI para una respuesta eficaz.

ESS02.05 Resolver y recuperarse ante incidentes. - Documentará, solicitará y probará las soluciones a los incidentes reportados y ejecutará procedimientos para la recuperación de los servicios tecnológicos.

Aplicará las soluciones más adecuadas a los problemas reportados; analizará el tipo de solución que se aplicó para resolverlo; tomará acciones en caso de ser necesaria una recuperación; y comunicará y documentará la solución empleada.

ESS02.06 Cerrar peticiones de incidentes y servicios. - Validará la satisfacción de los usuarios una vez que se haya cerrado el incidente reportado.

Verificará con el usuario el cierre de la incidencia, (si así fue acordado) una vez que el mismo se encuentre totalmente solventado; y ejecutará el cierre de la misma.

ESS02.07 Seguir el estado y emitir informes. - Realizará el seguimiento de los incidentes reportados con el fin de mantener la información necesaria para satisfacer el proceso de mejora continua de la unidad de TI y la atención al usuario.

Supervisará los casos que han sido abiertos con respecto a los servicios de TI y las soluciones que los han solventado; identificará la frecuencia con la que se presentan dichos problemas; identificará patrones recurrentes, así cono niveles de servicio ineficientes; y dispondrá de reportes con acceso controlado que permitan generar informes.

3.4.3 ESS03 Administrar los Problemas

La unidad encargada de las Tecnologías de la Información deberá identificar los problemas, las causas y buscará soluciones adecuadas para evitar que dichos eventos sean recurrentes.

ESS03.01 Identificar y clasificar problemas. - Establecerá procedimientos que incluyan la clasificación y priorización de los eventos para mantener informados a los interesados sobre los problemas identificados.

Definirá niveles de priorización de los problemas a través de la correlación de eventos y registros de incidentes; administrará de una manera formal los requerimientos, incidentes y problemas generados en los servicios de ti y accesos a la información importante como gestión de configuraciones, cambios y activos de TI; determinará el personal idóneo para formar equipos de trabajo que puedan identificar los problemas y proponer soluciones a los mismos; revisará los SLAs para definir las prioridades antes los problemas que pueden suscitarse; mantendrá informados a los usuarios sobre las soluciones a los problemas reportados mediante mecanismos oportunos como mesa de ayuda.

ESS03.02 Investigar y diagnosticar problemas. - Utilizará el criterio y la experiencia del personal de la unidad de TI en temas relevantes para identificar los problemas y las causas que los generan.

Comparará los errores que se generen con los almacenados en la base de conocimiento; asociará éstos eventos con las configuraciones que se encuentren afectadas; e informará sobre el avance de las posibles soluciones con el objetivo de medir el impacto que causaron en la entidad.

ESS03.03 Levantar errores conocidos. –Identificará las causas raíz de los problemas y creará un registro en la base de conocimiento con la solución temporal o definitiva.

Establecerá una solución temporal al problema para identificar, evaluar y priorizar una solución definitiva para minimizar el impacto en la entidad.

ESS03.04 Resolver y cerrar problemas. – Iniciará la ejecución de una solución a la causa raíz, solicitando el cambio al proceso de gestión de cambios referente a errores; manteniendo informados a los servidores o funcionarios sobre las acciones que se tomarán para ejecutar la solución.

Cerrará los registros de los problemas reportados una vez que se haya confirmado que la solución aplicada fue satisfactoria; informará a los usuarios involucrados sobre la solución que se pondrá en marcha y el tiempo que tomará el servicio en volver a la normalidad; generará informes de forma periódica sobre los problemas que se presenten y la solución de los mismos; verificará el impacto que producen los eventos suscitados en los servicios tecnológicos.

ESS03.05 Realizar una administración de problemas proactiva. – Identificará tendencias de problemas a través de la revisión de datos operacionales y emitirá una valoración de éstas.

Almacenará la información sobre los problemas que tengan relación con el control de cambios y coordinará reuniones con los servidores o funcionarios implicados para identificar posibles soluciones y planificar cambios futuros; revisará con las autoridades los costos que se han derivado de los problemas presentados; escalará los problemas conforme se han definido en

los acuerdos de nivel de servicios; optimizará el uso de los recursos minimizando las soluciones temporales; e implantará soluciones definitivas con ayuda de la gestión de cambios.

3.4.4 ESS04 Administrar la Continuidad

La unidad de Tecnología de la Información elaborará un plan de continuidad que le permita responder a incidentes e interrupciones de servicio para brindar una operación continua de los procesos críticos para la entidad y los servicios TI requeridos; y mantener la disponibilidad de la información a un nivel aceptable para la entidad.

ESS04.01 Definir la política de continuidad de negocio, objetivos y alcance. - Definirá la política y alcance de continuidad de la institución alineada con los objetivos de la entidad y de las partes interesadas.

Identificará los interesados clave, los procesos de negocio esenciales y las actividades de servicio de TI que son críticas para las operaciones de la entidad, con el objetivo de definir los roles y responsabilidades en la política de continuidad y su alcance.

ESS04.02 Mantener una estrategia de continuidad. - Evaluará las opciones de manejo de la continuidad de negocio y seleccionará una estrategia de continuidad viable y efectiva en costos, que permita asegurar la continuidad y recuperación de los servicios de TI mediante estrategias de negocio y opciones técnicas en la entidad frente a un desastre, disrupción u otro incidente mayor, tomando en cuenta la seguridad de la información.

Identificará posibles escenarios y amenazas que puedan causar incidentes y/o pérdidas de continuidad del negocio e identificará medidas que puedan reducir la probabilidad y el impacto, mejorando la prevención; realizará un análisis de riesgos para evaluar el impacto en tiempo de una disrupción en funciones críticas de la entidad y el efecto que tendría; establecerá tiempos mínimos para recuperar un servicio de TI basándose en una duración aceptable de interrupción;

y pondrá en conocimiento de la autoridad correspondiente las opciones estratégicas seleccionadas para su aprobación.

ESS04.03 Desarrollar e implementar la continuidad del negocio. – Considerará el desarrollará de un plan de continuidad de negocio (BCP) basado en la estrategia y procedimientos definidos para el uso en un incidente, con el fin de facilitar que la entidad continúe con sus actividades críticas y disponga de un sitio de procesamiento alterno.

Definirá las acciones y comunicaciones de respuesta a incidentes que deben ser ejecutadas en un evento de perdida de continuidad del negocio, con roles y responsabilidades; desarrollará y mantendrá planes de continuidad que contengan los recursos necesarios (personas, instalaciones e infraestructura de TI) y procedimientos que deben ser seguidos para continuar operando los procesos críticos de negocio y su recuperación hasta la reanudación de los procesos de negocio, incluyendo la actualización y conciliación de las bases de datos para preservar la integridad de la información. Definirá y documentará los requerimientos de información de respaldo para soportar los planes; y difundirá los planes y documentación de soporte a las partes interesadas y autorizadas y se asegurará que estén accesibles en escenarios de desastre.

ESS04.04 Ejercitar, probar y revisar el BCP. - Ejecutará periódicamente los planes de recuperación, para permitir el desarrollo de soluciones innovadoras y para verificar que el plan funcionará, en el tiempo, como se espera.

Definirá objetivos para ejercitar y probar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de la entidad, validará los procedimientos de continuidad, e incluirá roles y responsabilidades para realizar ejercicios y pruebas planificas del plan de continuidad, realizará un análisis y revisión post-ejercicio que permita incluir

recomendaciones para mejorar el plan de continuidad actual en base a los resultados de la revisión.

ESS04.05 Revisar, mantener y mejorar el plan de continuidad. - Revisará y evaluará periódicamente el plan de continuidad para asegurar su continua idoneidad, adecuación y efectividad. Incluirá control de cambios asegurando que el plan de continuidad se mantenga actualizado con los requerimientos y objetivos de negocio actuales, tanto estratégicos como operativos.

Revisará el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: la organización de la entidad, los procesos de negocio, los acuerdos de externalización, las tecnologías, la infraestructura, los sistemas operativos y los sistemas de aplicaciones; y comunicará los cambios realizados en los planes, procedimientos, infraestructura, roles y responsabilidades para su aprobación mediante el proceso de control de cambios.

ESS04.06 Proporcionar formación en el plan de continuidad. – Brindará capacitaciones regulares que incluyan los procedimientos y sus roles y responsabilidades en caso de pérdida de la continuidad a todas las personas implicadas tanto internas como externas.

Definirá y evaluará los planes de capacitación basados en formación práctica que incluyan la participación en ejercicios y las pruebas para quienes realicen planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes.

ESS04.07 Administrar acuerdos de respaldo. – Definir procedimientos para mantener la disponibilidad en el tiempo de la información crítica del negocio; así como los mensajes y archivos firmados electrónicamente.

Realizará copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida y aprobada, considerando al menos frecuencia (mensual, semanal, diaria, etc.), modo de copias de seguridad (por ejemplo; cintas, discos espejo, DVD-ROM), tipo de copias de seguridad (completa, diferencial, incremental), localización física y lógica de las fuentes de los datos, seguridad y derechos de acceso y cifrado a ser aplicado, en función de los requerimientos del almacenamiento de las copias de seguridad, dentro y fuera de la propia ubicación, que satisfagan el cronograma y los requerimientos definidos y aprobados de la entidad; y realizará pruebas de la integridad de la información contenida en las copias de seguridad periódicamente.

3.4.5 ESS05 Administrar Servicios de Seguridad

La unidad de Tecnología precautelará, protegerá y salvaguardará contra pérdidas la información de la entidad, de manera que permita mantener un nivel de riesgo de seguridad de la información aceptable de acuerdo con la política de seguridad. Establecerá y mantendrá los roles de seguridad y privilegios de acceso a la información y realizará la supervisión de la seguridad.

ESS05.01 Proteger contra software malicioso (malware). - Implementará y mantendrá medidas de prevención, detección y corrección (parches de seguridad actualizados y control de virus actualizados periódicamente) con el fin de proteger los sistemas informáticos del software malicioso (virus, gusanos, software espía –spyware- correo basura, otros).

Ejecutará programas de concientización sobre el software malicioso en el uso del Internet y el correo electrónico, establecerá procedimientos de prevención, implementará herramientas centralizadas de protección de software malicioso, filtrará el tráfico entrante de correos

electrónicos y descargas para protección de los equipos informáticos; y restringirá el uso de programas utilitarios que puedan manipular el sistema de forma manual.

ESS05.02 Gestionar la seguridad de la red y las conexiones. - Definirá e implementará medidas de seguridad y procedimientos para proteger la información en cualquier modo de conexión y transmisión a través de la red, incluyendo los proyectos nuevos de TI que cuenten con requerimientos de red, así como acuerdos para la transmisión segura de información incluyendo los datos enviamos mediante correo electrónico institucional.

Establecerá una política de seguridad que deberá ser actualizada y aprobada por la autoridad correspondiente de forma periódica, a través de un análisis de riesgos y los requerimientos de la entidad, para permitir el acceso a la información a través de un inicio de sesión seguro y a la red exclusivamente a dispositivos autorizados mediante el uso de contraseñas y protocolos de seguridad, que deben mantener la calidad de las claves, cifrará la información confidencial antes de ser transmitida; segregará las redes de comunicaciones; y realizará pruebas de intrusión y seguridad periódicas, que permitan determinar el nivel de protección de la red y del sistema.

ESS05.03 Gestionar la seguridad desde los puestos del usuario final. – En la política de seguridad de la información definirá un apartado con el que asegurará que los equipos (computador portátil, computador fijo, equipo servidor y otros dispositivos y software móviles y de red) conforme los requerimientos de seguridad de la información procesada, almacenada o transmitida.

Configurará los sistemas operativos de forma segura, implementará mecanismos de bloqueo de los dispositivos, cifrará la información almacenada en los equipos de acuerdo a su clasificación, gestionará el acceso y el control remoto; validará que los proyectos cuenten con

seguridades de usuario final; y proveerá medidas de seguridad tanto dentro como fuera de la entidad.

ESS05.04 Gestionar la identidad del usuario y el acceso lógico. - Asegurará que los usuarios tengan cuentas estandarizadas de identificación con permisos de acceso a la información alineadas con sus funciones, horarios y coordinará con las unidades de negocio su revisión y actualización periódica.

Administrará los accesos (creación, modificación y eliminación) de los usuarios debidamente identificados mediante roles, basándose en pedidos documentados y autorizados por la autoridad correspondiente conforme lo definido en la política de seguridad de la entidad, realizará revisiones periódicas de las cuentas y sus privilegios, segregará y gestionará cuentas de usuario privilegiadas, asegurará que los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) sean identificables y respaldadas; incluirá dentro de la política de seguridad de la información la definición y el uso de controles criptográficos; en caso de tratarse de un nuevo proyecto verificará las definiciones de los accesos para asegurar la información; y mantendrá pistas de auditoría de los accesos a la información clasificada como altamente sensible.

ESS05.05 Gestionar el acceso físico a los activos de TI. - Definirá e implementará procedimientos para conceder, limitar y revocar accesos físicos de acuerdo con las necesidades de la entidad, mismos que deberán formar parte de la política de seguridad. Los accesos concedidos deberán estar justificados, autorizados, registrados y supervisados, lo que aplicará a empleados fijos y temporales, clientes, vendedores, visitantes e integrantes de los proyectos de TI.

Gestionará los accesos a las instalaciones de procesamiento de información, mediante peticiones documentales y formales de acceso, debidamente autorizadas por la unidad de TI, detallando las áreas a las que se le ha concedido acceso (centro de datos, áreas de servidores, oficinas, edificios) según las funciones y responsabilidades asignadas.

ESS05.06 Administrar documentos sensibles y dispositivos de salida. - Establecerá protecciones físicas apropiadas, prácticas de contabilidad y control del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial, credenciales (token) de seguridad y dispositivos móviles que contengan información confidencial.

Definirá procedimientos para administrar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, incluyendo dispositivos móviles, token (firma digital, etc.), los cuales deberán estar considerados en la política de seguridad de la información, elaborará un inventario de documentos sensibles y dispositivos de salida y lo conciliará regularmente, asignará privilegios de acceso a estos documentos sensibles y dispositivos de salida usando el principio del menor privilegio, destruirá la información sensible y protegerá los dispositivos de salida (por ejemplo, desmagnetizar soportes magnéticos, destruir físicamente dispositivos de memoria, usar trituradoras para destruir documentos confidenciales).

ESS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad. - Usará herramientas de detección de intrusiones, supervisará la infraestructura para detectar accesos no autorizados y asegurará que cualquier evento esté integrado con la gestión de incidentes.

Registrará y analizará periódicamente eventos relacionados con la seguridad, reportados por las herramientas de monitoreo de seguridad de la infraestructura, creará tickets de incidentes

de seguridad cuando el monitoreo identifique potenciales incidentes de seguridad y definirá un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales, informando a todos los servidores que se encuentran expuestos a éstos incidentes.

3.4.6 ESS06 Administrar Controles de los Procesos del Negocio

La unidad de Tecnología definirá y aplicará controles para brindar integridad a la información de la entidad, así como seguridad a los activos de la información manejados en los procesos del negocio.

ESS06.01 Alinear los controles de los procesos con los objetivos institucionales. - Evaluará y supervisará periódicamente los controles aplicados en la ejecución de las actividades de los procesos de negocio, para asegurar que los controles están alineados con las necesidades de la entidad.

Definirá y supervisará los controles de los procesos claves de la entidad para conseguir los objetivos estratégicos, de cumplimiento y operacionales, priorizará y verificará continuamente el diseño y operación de los controles basados en el riesgo inherente del negocio en busca de oportunidades de mejora.

ESS06.02 Controlar el análisis de los datos. - Manejará la ejecución de las tareas de los procesos de la entidad y los controles relacionados, certificando que el análisis de los datos es válido, completo, preciso, oportuno y seguro.

Implementará métodos de autenticación de las transacciones y verificará la existencia de autoridad para originar las mismas en el momento oportuno, mantendrá integridad de los datos asegurando que las transacciones erróneas no interrumpan el procesamiento de las válidas,

precautelará la confidencialidad de la información de forma precisa y completa mediante la entrega al beneficiario autorizado.

ESS06.03 Administrar roles, privilegios y niveles de autorización. – Establecerá roles y segregación de funciones, autorizará el acceso a los activos de información, incluyendo los que cuentan con terceras partes, asegurando que la entidad sabe quién tiene acceso a la información y quien la está manejando.

Asignará y revisará continuamente los roles, responsabilidades y niveles de autoridad para la aprobación de transacciones, realizará capacitación periódica para que todos los usuarios entiendan sus responsabilidades; así como la importancia de los controles; y las propiedades que deben mantenerse sobre la información: integridad, confidencialidad y privacidad.

ESS06.04 Administrador Errores y excepciones. – Monitoreará las excepciones y errores de los procesos de negocio con niveles de escalamiento que faciliten la ejecución de acciones correctivas definidas, brindando integridad a la información del negocio.

Definirá procedimientos para monitorear, revisar, informar, corregir errores, remplazar errores y excepciones y realizará seguimiento de las medidas correctivas aplicadas.

ESS06.05 Asegurar responsables y activos de la información. – Certificará que la información de la entidad puede ser rastreada hasta quien la originó y los eventos producidos con la misma y definirá procedimientos como uso de firma electrónica que permita asegurar los activos de información accesibles por la entidad.

Aplicará e implementará procedimientos, herramientas y políticas de clasificación, etiquetado y manejo de los activos, con el fin de proteger la información crítica de la entidad; limitará el uso, repartición y el acceso a la información según su clasificación; informará periódicamente a la entidad y los interesados sobre violaciones y desviaciones encontradas;

implementará los medios necesarios para facilitar el uso de firma electrónica, incluirá reportes de auditoría sobre los mensajes firmados electrónicamente; y validará que la institución que emite el token esté acreditada y autorizada.

3.5 Supervisar, Evaluar y Valorar (SEV)

Este dominio cuenta con 3 procesos que, mediante la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio, la aplicación del gobierno, las mediciones y el control permanente busca garantizar la eficiencia operativa y detectar oportunidades de mejora a los procesos que maneja el área de TI.

3.5.1 SEV01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad

La unidad de Tecnologías de la Información recolectará, validará y evaluará métricas y objetivos de negocio, de TI y de procesos; supervisará que los procesos se estén realizando conforme a los objetivos y métricas; y se proporcionen informes de forma sistemática y planificada.

SEV01.01 Establecer un enfoque de la supervisión. - Identificará e involucrará a las partes interesadas en un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio.

Identificará a las partes interesadas, mantendrá y alineará de forma continua el enfoque de supervisión y evaluación, así como las herramientas utilizadas para la obtención de datos y presentación de informes corporativos (por ejemplo: aplicaciones de inteligencia de negocio), validará periódicamente el enfoque utilizado e identificará los nuevos grupos de interés, requisitos y recursos.

SEV01.02 Establecer objetivos de cumplimiento y rendimiento. - Revisará y actualizará periódicamente en conjunto con las partes interesadas la definición y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento.

Definirá y revisará periódicamente los objetivos y métricas con las partes interesadas para definir la razonabilidad de metas y tolerancias; comunicará los cambios propuestos en las metas y tolerancias de rendimiento y cumplimiento (referidos a las métricas) con las partes interesadas; y evaluará si los objetivos y métricas son adecuados, es decir, específicos, medibles, alcanzables, relevantes y limitados en el tiempo.

SEV01.03 Recopilar, analizar y supervisar datos de cumplimiento y rendimiento. - Recopilará y analizará datos oportunos y precisos de acuerdo con los objetivos de la entidad, e informará de forma periódica sobre el desempeño respecto de los objetivos

Recopilará datos de los procesos definidos, de forma automatizada, cuando sea posible; consolidará los datos para soportar el cálculo de las métricas; y alineará los datos consolidados a los enfoques y objetivos de presentación de información de la entidad. Diseñará informes de rendimiento de procesos que sean concisos y ajustados a las diferentes necesidades de gestión y audiencias, facilitando la toma efectiva y oportuna de decisiones (por ejemplo: cuadros de mando, informes con semáforos); recomendará cambios a los objetivos y métricas, cuando sea procedente; hará seguimiento de los resultados de las acciones comprometidas, e informará de los resultados a las partes interesadas.

3.5.2 SEV02 Supervisar, Evaluar y Valorar el sistema de Control Interno

La unidad de Tecnologías de la Información supervisará de forma continua el entorno de control apoyándose en evaluaciones externas con el objetivo de identificar deficiencias en el

control existente e implementar procesos de mejora de las mismas; y mantendrá normas para la evaluación de control interno.

SEV02.01 Supervisar el control interno. - Supervisará continuamente la mejora del entorno de control de TI y el marco de control existente para alcanzar los objetivos institucionales, incluirá revisión de temas relacionados con seguridad de la información.

Realizará actividades de control interno basándose en estándares de gobierno y marco de referencia y mejores prácticas reconocidas; considerará la evaluación realizada por las auditorías; identificará las limitaciones que posee el sistema de control interno de la entidad; asegurará que las actividades de control están operativas y que las excepciones sean comunicadas con oportunidad y dará seguimiento; mantendrá las revisiones de control interno tomando en cuenta los cambios en la entidad y los riesgos de TI; realizará estudios comparativos de estándares aceptados para evaluar el rendimiento del control interno.

SEV02.02 Examinar la efectividad de los controles que tienen los procesos de la entidad. – Revisará las evidencias y pruebas realizadas de los controles existentes de forma periódica y continua para validar la eficacia y efectividad de los controles existentes en la entidad; y el cumplimiento de los controles definidos en la política de seguridad de la información.

Priorizará los riesgos de acuerdo a los objetivos de la entidad; identificará los controles clave y los validará: y mantendrá evidencia de la efectividad de los controles implementados.

SEV02.03 Realizar autoevaluaciones de control. – Concientizará a los dueños de los procesos sobre la importancia de posesionarse sobre los controles y sus mejoras.

Desarrollará criterios de autoevaluación periódicos; asignará responsables para asegurar la objetividad; incentivará la ejecución de revisiones independientes; coordinará las evaluaciones

con auditores internos o externos; y comunicará los resultados de las autoevaluaciones para considerar acciones correctivas.

SEV02.04 Identificar y comunicar las deficiencias de control. – Identificará las deficiencias de control, analizará sus causas y las escalará a las partes interesadas.

Identificará, comunicará y registrará las excepciones de controles y asignará a los responsables de su solución; realizará seguimiento a las excepciones de que se han tomado acciones sobre las mismas.

SEV02.05 Garantizar que los proveedores de aseguramiento son independientes y están calificados. – Asegurará que quien realiza el aseguramiento es independiente de la entidad, y que poseen el conocimientos profesionales y experiencia adecuada para cumplir con las funciones encomendadas.

Establecerá la lealtad que deben cumplirse con respecto al código de ética y a los estándares aplicables; establecerá independencia con los proveedores de aseguramiento; y definirá las competencias que deben poseer los proveedores.

SEV02.06 Planificar, estudiar y ejecutar iniciativas de aseguramiento. – Planificará, definirá y ejecutará las iniciativas de aseguramiento tomando como base las prioridades de la estrategia y los objetivos de la entidad e informará sobre los hallazgos que se identifiquen y realizará recomendaciones de mejora sobre los riesgos encontrados.

Definirá el objeto de las revisiones; ejecutará una evaluación de riesgos y verificará la capacidad de los procesos con los que diagnostica los riesgos; seleccionará los procesos que serán los objetos de control; definirá el alcance actual identificando los objetivos, los procesos y recursos de TI y las unidades auditables; establecerá el plan y los recursos necesarios; detallará los procedimientos para recolectar y evaluar la información; instaurará métodos para la

definición de controles y resultados; medirá los riesgos residuales; clasificará el alcance de los objetivos de controles clave sobre aseguramiento de TI; verificará la efectividad de los controles y probará sus resultados; documentará las debilidades y el impacto que causan; mantendrá comunicación con las autoridades para que exista aprobación sobre los hallazgos y las recomendaciones; asegurará que el trabajo de aseguramiento se lo realice completo; e informará a las autoridades sobre los temas clave y las acciones primordiales.

3.5.3 SEV03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

La unidad de Tecnologías de la Información evaluará el cumplimiento de requisitos legales y contractuales en los procesos de TI y de la entidad, validando que se cumplan de forma general.

SEV03.01 Identificar requisitos externos de cumplimiento y optimizar la respuesta. - Evaluará continuamente cambios en las leyes nacionales y otros requisitos del área de TI; revisará las políticas, principios, estándares y metodologías para la administración de requisitos legales y regulatorios para mantener la eficacia y eficiencia en el aseguramiento del cumplimiento; y comunicará nuevos requerimientos y las modificaciones semestrales.

Asignará responsables para la supervisión de cambios legales sobre requisitos de TI y el procesamiento de información; identificará los requisitos de cumplimiento y el impacto que podrían tener en la entidad; valorará el impacto de los requisitos relacionados con proveedores de la entidad; obtendrá el asesoramiento correspondiente en caso de ser necesario; mantendrá un inventario sobre requisitos legales, su impacto y las acciones a realizar.

SEV03.02 Confirmar el cumplimiento de requisitos externos y obtener garantía sobre los mismos. - Revisará el cumplimiento de regulaciones legales; obtendrá garantías de

cumplimiento de políticas y estándares; y confirmará que se cerraron a tiempo las acciones correctivas para tratar diferencias.

Evaluará regularmente las políticas, procedimientos y estándares de todas las funciones corporativas; administrará las deficiencias sobre el cumplimiento de las políticas; evaluará de forma periódica para asegurar el cumplimiento legal; detectará patrones reiterados en el fallo de cumplimiento; evidenciará regularmente el cumplimiento de las políticas internas; probará tanto interna como externamente los niveles de cumplimiento; analizará el cumplimiento de las regulaciones legales por parte de los proveedores; supervisará el incumplimiento de las leyes; y consolidará a nivel de entidad los requisitos, etc.

3.6 RESUMEN CONTENIDO NORMATIVA PROPUESTA

Tabla 16:

Controles contenidos en normativa propuesta

CONTROLES NORMATIVA PROPUESTA			**NORMAS RELACIONADAS**		
Dominio	**Proceso Propuesto**	**Nombre Proceso propuesto**	**Relación NCI**	**Relación ISO 27002**	**Relación ITIL V3**
Evaluar, Orientar y Supervisar	EOS01	Establecer y mantener el marco de Gobierno		17.1	
	EOS02	Aseverar la Entrega de Beneficios			SS4
	EOS03	Asegurar la Optimización del Riesgo			
	EOS04	Asegurar la Optimización de los Recursos			SS3
	EOS05	Asegurar la Transparencia hacia las partes interesadas			
Alinear, Planificar y Organizar	APO01	Administrar el marco de gobierno de TI	NCI 410-01, NCI 410-16, NCI 410-02, NCI 410-04	6.1, 6.2, 7.2, 5.1, 8.1, 6.1, 14.2, 5.1	CSI2
	APO02	Administrar la estrategia	NCI 410-03	6.1	SS1
	APO03	Administrar la arquitectura de la entidad	NCI 410-05	14.2, 12.7, 14.1, 14.2, 18.1	
	APO04	Administrar la innovación	NCI 410.14, NCI 410-17	12.1, 17.2, 6.1, 6.2	
	APO05	Administrar el portafolio			SS4, SD1
	APO06	Administrar los recursos humanos	NCI 410-15, NCI 410-17	7.1, 14.2, 15.2, 7.2, 12.1, 7.2, 18.1, 8.2, 9.3, 13.2	SD3

CONTROLES NORMATIVA PROPUESTA			NORMAS RELACIONADAS		
Dominio	**Proceso Propuesto**	**Nombre Proceso propuesto**	**Relación NCI**	**Relación ISO 27002**	**Relación ITIL V3**
	APO07	Administrar los acuerdos de servicio	NCI 410-12, NCI 410-13	14.2	SS4, SD1, SD2, CSI1
	APO08	Administrar los proveedores	NCI 410-07, NCI 410-08	13.2, 15.1, 15.2	SD7
	APO09	Administrar la calidad			
	APO10	Administrar el riesgo	NCI 410-11		SD6
	APO11	Administrar la seguridad			
Construcción, Adquisición e Implementación	CAI01	Administrar Programas y Proyectos	NCI 410-06	6.1	
	CAI02	Administrar la definición de requisitos	NCI 410-07		SD2
	CAI03	Administrar la identificación y construcción de soluciones	NCI 410-07, NCI 410-08, NCI 410-09	7.2, 13.2, 14.2 , 4.3	
	CAI04	Administrar la disponibilidad y la capacidad	NCI 410-12		SD3, SD4
	CAI05	Administrar cambios organizativos			
	CAI06	Administrar los cambios			ST2
	CAI07	Administrar la aceptación del cambio y la evolución	NCI 410-09, NCI 410-12	13.2, 14.2	ST1, ST6, ST4, ST5
	CAI08	Administrar el conocimiento			ST7
	CAI09	Administrar los activos	NCI 410-09	7.3, 8.1, 8.3, 8.1	ST3
	CAI10	Administrar la configuración			ST3
Entregar, dar Servicio y Soporte	ESS01	Administrar Operaciones	NCI 410-10	12.1, 12.4, 12.5, 12.6, 8.1, 9.1, 11.1, 11.2	SO1
	ESS02	Administrar Peticiones e Incidentes de Servicio		16.1	SO2, SO3

CONTROLES NORMATIVA PROPUESTA			NORMAS RELACIONADAS		
Dominio	**Proceso Propuesto**	**Nombre Proceso propuesto**	**Relación NCI**	**Relación ISO 27002**	**Relación ITIL V3**
	ESS03	Administrar los Problemas		12.6, 16.1, 11.2,	SO4
	ESS04	Administrar la Continuidad	NCI 410-10, NCI 410-11, 410-17		SD5
	ESS05	Administrar Servicios de Seguridad	NCI 410-10, NCI 410-12, NCI 410-17	9.4, 12.2, 5.1, 6.1, 8.3, 9.1, 9.3, 12.1, 12.4, 13.1, 13.2, 14.1, 18.1, 5.1, 6.1, 11.2, 6.2, 9.2, 10.1, 9.1, 11.1, 6.2, 7.3, 8.1, 16.1	
	ESS06	Administrar Controles de los Procesos del Negocio	NCI 410-17	8.1, 8.2	SD6
Supervisión, Evaluación y Verificación	SEV01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad			
	SEV02	Supervisar, Evaluar y Valorar el sistema de Control Interno		18.2, 5.1	
	SEV03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		18.1	CSI2
Total Procesos:		**35**	**17**	**35**	**23**

Nota: Elaborada por los autores, Figueroa F., Hinojosa L.

La Propuesta de normativa para el Control Interno de T.I. al estar basada en COBIT, contiene los marcos VAL IT, RISK IT, además se consideró la inclusión de las Normas de Control Interno vigentes, así como la inserción de los controles constantes en la Norma ISO 27002:2103 y las prácticas de ITIL v3, el detalle se encuentra ampliado en el Anexo A.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- La Asamblea Nacional del Ecuador aprobó en el 2015 la enmienda constitucional con la que le retiró la potestad de revisar el cumplimiento de los objetivos institucionales a la Contraloría General del Estado; por lo que, el desarrollo de la Propuesta de Normativa basada en COBIT 5 para el Control Interno de Tecnologías de la Información del sector Público Ecuatoriano no incluyó controles que tengan relación con la gestión orientada al cumplimiento de objetivos de la entidad; sin embargo, es una propuesta completa y aplicable en todas las entidades públicas sin discriminar su tamaño.
- Al analizar los estándares internacionales y las mejores prácticas sobre controles tecnológicos, utilizando matrices comparativas frente al marco de referencia COBIT 5 se evidenció que éste es un marco completo e integral que abarca estándares como RISK IT, VAL IT, que se complementa con el uso de los controles contenidos en ITIL, COSO, IS027002, así como las Normas de Control Interno vigentes, haciendo de esta manera que la propuesta de normativa de control interno contenga controles idóneos y aplicables en el sector público ecuatoriano y factible de aportar con revisiones de cumplimiento por los entes de control y utilizable en la identificación de recomendaciones de mejora para las falencias encontradas.
- Una vez desarrollados los controles basados en COBIT para las entidades del sector público ecuatoriano se observó que las Normas de Control Interno que están vigentes en la Contraloría General del Estado mantienen vacíos debido al crecimiento tecnológico, lo que ocasiona que existan vacíos legales que pueden ser llenados los

controles propuestos y que serán útiles para establecer recomendaciones de prevención, corrección y mejora en todas las entidades.

- El vacío legal existente en el grupo 410 TECNOLOGÍAS DE LA INFORMACIÓN de las Normas de Control Interno referente a políticas de control y administración de accesos de los usuarios, autenticación, redes y servicios asociados, protección de información confidencial, gestión de contraseñas, seguridad del cableado, salida de equipos, gestión de vulnerabilidades técnicas, mecanismos de seguridad asociados a servicios de red, segregación de redes, política de desarrollo seguro de software, respuesta a los incidentes de seguridad, regulación de los controles criptográficos entre otros, es cubierto en su totalidad gracias a los controles desarrollados en esta propuesta de Normativa de Control Interno, basada en COBIT 5, permitiendo establecer recomendaciones de prevención, corrección y mejora en todas las entidades del sector público ecuatoriano de cumplimiento obligatorio.

4.2 Recomendaciones

- Se recomienda que la Contraloría General del Estado tome como punto de partida esta Propuesta de Normativa basada en COBIT 5, Val IT, Risk IT, COSO, ITIL; así como las Normas Internacionales ISO e ISSAI para el Control Interno de Tecnologías de la Información del sector Público Ecuatoriano para elaborar una actualización de su grupo 410 TECNOLOGÍA DE LA INFORMACIÓN, de manera que llene los vacíos legales existentes en la normativa de control interno vigente, con la incorporación de este compendio de controles actuales e idóneos a la realidad ecuatoriana y aplicadas en las entidades del sector público para que los funcionarios encargados de las revisiones de control cuenten con las herramientas suficientes para la ejecución de las acciones de control.

- Es recomendable que esta propuesta de normativa basada en COBIT 5, para el Control Interno de tecnologías de la información del sector público ecuatoriano se ponga en marcha mediante la ejecución de una evaluación de control interno en entidades del sector público de tamaño distinto, con el fin de medir las mejoras propuestas a la normativa vigente; y se valide la identificación de vulnerabilidades y la posibilidad de que el ente de control emita recomendaciones de mejora en políticas de control y seguridad de la información y la prestación de servicios tecnológicos.

Bibliografía

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *4*(2), 92–100. https://doi.org/10.4236/jis.2013.42011

Espinoza Pamela. (2013). Gobierno de TI | Val IT. Retrieved November 30, 2017, from http://pamela7913.wixsite.com/pamvic/val-it

Galaz y Yamazaki y Ruiz, S. C. (2015). COSO Marco de referencia para la implementación, gestión y control de un adecuado Sistema de Control Interno, 23.

Gmacagno. (2013). COSO II Internal Control Integrated Framework.

Grupa, P. (2015a). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. Retrieved November 8, 2017, from http://www.iso27000.es/iso27000.html

Grupa, P. (2015b). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. Retrieved November 8, 2017, from http://iso27000.es/iso27002.html

Hardy, H. J. (2008). *Alineando COBIT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio de la empresa*. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

Instituto de Auditores Internos, E. (2013). Control Interno - Marco Integrado. *Control Interno*.

International Standarization Organization. (2014). *Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary* (Third edit, Vol. 2014).

INTOSAI. (2013). *Information System Security Review Methodology*. Copenhague.

INTOSAI. (2015). Principios Fundamentales de Auditoría del Sector Público.

ISACA. (2006). *Valor para la empresa: Buen gobierno de las inversiones en TI el caso de negocio*.

ISACA. (2008). *Enterprise Value: Governance of IT Investments*.

ISACA. (2009a). *Marco de Riesgo de TI, español*. 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA.

ISACA. (2009b). *The Risk IT Framework*. https://doi.org/978-1-60420-116-1

ISACA. (2012a). COBIT5-Introduction-Spanish.

ISACA. (2012b). *Un marco de negocio para el Gobierno y la Gestión de la Empresa, COBIT 5*.

ISACA. (2013). *Procesos Catalizadores*.

ISACA. (2014). Relating the COSO Internal Control— Integrated Framework and COBIT, 1–22.

Iso27000.es. (2013). ISO/IEC 27002:2013. Retrieved from http://iso27000.es/download/ControlesISO27002-2013.pdf

López y Molinal y Quintanilla, F. de M. (2008). *Procedimientos de Auditoría aplicados a los sistemas de información computarizados para la detención, prevención y corrección de los delitos informáticos*. Universidad de El Salvador.

Molina & Rodríguez & Sánchez &Vergel. (2012). Guía para la seguridad basada en la norma ISO/IEC 27002, para la dependencia División de Sistemas de la Universidad Francisco de Paula Santander Ocaña.

Neira, A. L., & Spohr, J. R. (2010). Sistema de Gestión de la Seguridad de la Información. *Article*, *1*.

Norma Técnica Ecuatoriana 27002:2009, 1 Tecnología de la información. Técnicas de la seguridad. Código de práctica para la gestión de la seguridad de la información § (2008).

Office of Government Commerce. (2009). *ITIL, estrategia del servicio, OGC*.

Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores, O. Carta constitutiva (2012).

Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores, O. (2015). Plan estratégico 2011-2015.

Páliz, V. M. (2017). *Propuesta de complemento al artículo 410 de la Norma de Control Gubernamental Moderno emitida en el año 2009 por la Contraloría General del Estado del Ecuador sobre las tecnologías de la información y comunicaciones, aplicando estándares y buenas práctica*. Instituto de Altos Estudios Nacionales.

Pólit, C. (Contralor G. del E. Normas de Control Interno para las Entidades, Organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos (2009).

Ríos, S. (2011). ITIL v3 Manual íntegro, 101. Retrieved from http://www.biable.es/wp-content/uploads/2014/ManualITIL.pdf

The Committee of Sponsoring Organizations of the Treadway Commission. (2013). COSO - Internal control / integrated framework executive summary. *Committe of Sponsoring Organisation of the Treadway Commission*, 1–8.

The Committee of Sponsoring Organizations of the Treadway Commission. (2017). The Committee of Sponsoring Organization (COSO). Retrieved August 15, 2017, from www.coso.org

Villacís, W. N. (2014). *Guía de evaluación de la gestión de TI con aplicación de COBIT y COSO en el sector público ecuatoriano*. Universidad de las Fuerzas Armadas - ESPE.