MAESTRÍA EN AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN

Modelo de evaluación de la gestión de Tecnología de Información basado en COBIT, ITIL, ISO 27002 y su efecto en la competitividad de las Cooperativas de Ahorro y Crédito de la zona y segmento 1

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por el estudiante:
Eduardo Patricio CANDO SALAS

Bajo la dirección de:
Raúl Vicente GONZÁLEZ CARRIÓN

Universidad Espíritu Santo
Maestría en Auditoría de Tecnologías de la Información
Samborondón - Ecuador
Abril de 2019

Modelo de evaluación de la gestión de TI basado en COBIT, ITIL, ISO 27002 y su efecto en la competitividad de COAC de la zona y segmento 1.

IT management evaluation model based on COBIT, ITIL, ISO 27002 and its effect on the competitiveness of COAC in the area and segment 1.

Eduardo Patricio CANDO SALAS[1]
Raúl Vicente GONZALEZ CARRIÓN[2]

RESUMEN

La implementación de las mejores prácticas debería ser consistente en la gestión de tecnología de la información (TI), basándose en un marco de control y gestión de riesgos integrándose con otras metodologías y prácticas en el cumplimiento de los requerimientos normativos de las Cooperativas de Ahorro y Crédito; el objetivo de esta investigación se centra en diseñar un modelo de evaluación de la gestión de TI, basado en los modelos de referencia COBIT 5, ITIL v3 e ISO 27002, para la determinación de la competitividad de las cooperativas en la zona y segmento 1; la metodología que se usó fue aplicativa, cualitativa, explorativa, bibliográfica y de caso de estudio en dos cooperativas del segmento 1, que por criterios de confidencialidad nombro por tamaño como GR grande y MD mediana. Se diseñó un modelo que contenga los criterios que se relacionen entre COBIT 5, ITIL v3 e ISO 27002, aplicado a las COACs de estudio, como principales resultados se obtuvieron: ninguna de las cooperativas cuenta con certificación ISO, las cooperativas caso de estudio y de validación están llegando a un promedio de madurez en la gestión de TI en un 58,44%, encontrándose mejor ubicadas la cooperativa GR y la B. Para la validación del instrumento se aplicó en tres cooperativas con características similares y del segmento 1, categorizadas como: A, B, y C, lo que permitió demostrar que el modelo propuesto es integral y se aplica a todo tipo de cooperativas del segmento 1 del Ecuador.

Palabras clave: | Cooperativa de Ahorro y Crédito, COBIT, evaluación, ISO, ITIL, Riesgo, Tecnología de Información.

ABSTRACT

The implementation of best practices should be consistent in the management of information technology (IT), based on a risk control and management framework integrated with other methodologies and practices in compliance with the regulatory requirements of the Savings Cooperatives and Credit; The objective of this research focuses on designing an IT management evaluation model, based on the reference models COBIT 5, ITIL v3 and ISO 27002, to determine the competitiveness of cooperatives in the zone and segment 1; The methodology used was applicative, qualitative, explorative, bibliographic and case study in two cooperatives of segment 1, which by confidentiality criteria named by size as large GR and medium MD. A model was designed that contains the criteria that are related between COBIT 5, ITIL v3 and ISO 27002, applied to the COACs of study, as main results were obtained: none of the cooperatives has ISO certification, the cooperatives case of study and validation are reaching an average maturity in IT management by 58.44%, with the GR and B cooperatives being better located. For the validation of the instrument, it was applied in three cooperatives with similar characteristics and segment 1, categorized as : A, B, and C, which allowed demonstrating that the proposed model is comprehensive and applies to all types of cooperatives in segment 1 of Ecuador.

Key words | Cooperativa de Ahorro y Crédito, COBIT, evaluation, ISO, ITIL, risk, IT.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador, e-mail ecando@uees.edu.ec
[2] CISA,CBCP,CICA,ISO22301 LI, ISO 22301 LA, ISO 27001 IA, COBIT, MSC. Docente de la Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador e-mail rgonzalesc@uees.edu.ec

INTRODUCCIÓN

En el Ecuador se promulgó la primera ley de cooperativas en el año de 1937, y a través de los años específicamente en el año 2011, el órgano legislativo ecuatoriano aprobó la Ley Orgánica de Economía Popular y Solidaria (LOEPS). Posterior a la ley que no solo derogó la Ley de Cooperativas de 1966 y la Ley de Entidades de Instituciones del Sistema Financiero de 1994, también unificó el control del sector cooperativo bajo una sola normativa, por lo que fue necesaria la promulgación de su Reglamento, esta acción se llevó a cabo en el ejecutivo, cuyo objetivo fue "establecer los procedimientos de aplicación de la Ley Orgánica de la Economía Popular y Solidaría y del Sector Financiero Popular y Solidario" (Asamblea Nacional, 2011).

Consecuentemente la Ley Orgánica de Economía Popular (LOEPS), determina controles y atribuciones diferenciadas para el sector asociativo y cooperativo (Superintendencia de Economía Popular y Solidaria (SEPS), 2018). La distribución geográfica de las organizaciones del sector no financiero por grupo, se refleja en la gráfica 1:

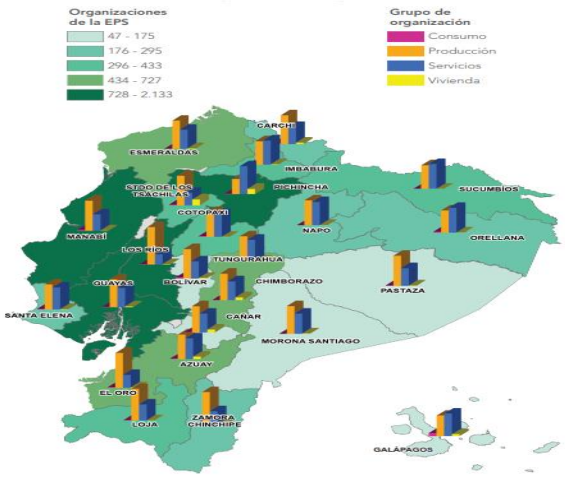


Gráfico 1. Distribución de Cooperativas
Fuente: SEPS, 2018

Tal es asi que la SEPS obtiene la responsabilidad del control y supervisión de las organizaciones de economía popular y solidaria en donde existen dos ámbitos importantes:

El sector financiero que se trata de todas las cooperativas de ahorro y crédito (COACs), organizaciones pequeñas como las cajas de ahorro, los bancos y cajas comunales.

El sector no financiero se encuentran las cooperativas de transporte, vivienda, consumo, producción, además de todas las asociaciones de producción y organizaciones comunales que realizan cualquier tipo de actividad económica y productiva (Arzbach, 2015)

Por otra parte es importante destacar que entre asociaciones y cooperativas que pertenecen al sector no financiero, suman 12.281 y ambos tipos de organizaciones basan sus relaciones en principios fundamentales como: la solidaridad, la cooperación, y la reciprocidad. De las 9.620 asociaciones, un 67% pertenecen a producción; el 32% a servicios; y el 1% a consumo. En tanto que de las 2.661 que son cooperativas, el 73% pertenecen a servicios; un 18% a producción; un 8% a vivienda; y el 1% a consumo.

Según la SEPS, existe un crecimiento acelerado en el sector y que corresponde al doble que actualmente registra el sector bancario, por lo que es un ejemplo de la redistribución de la riqueza y la prevalencia de lo colectivo sobre lo individual. Con determinacion existen 6 millones de socios en aproximadamente 600 cooperativas de ahorro y crédito, cajas y bancos comunales en el territorio ecuatoriano, con una administracion de los activos y su crecimiento por más de $11 mil millones y los pasivos que superan los $10 mil millones (SAAC, 2018)

En el caso del sector financiero para un mejor control y tratamiendo de las entidades del sector financiero se crea la segmentación por tamaño en sus activos y se divide en:

Tabla 1.- Clasificación de Segmentos por Valorización de Activos.

SEG	ACTIVOS (USD)
1	Mayor a 80´000 000,00
2	Mayor a 20´000 000,00 hasta 80´000 000,00
3	Mayor a 5´000 000,00 hasta 20´000 000,00
4	Mayor a 1´000 000,00 hasta 5´000 000,00
5	Hasta 1´000 000,00 Cajas de Ahorro, bancos comunales y cajas comunales

Fuente. - Superintendencia de Economía Popular y Solidaria, 2015

El sector financiero en el país juega un papel muy importante, es asi que las entidades reguladoras apoyan en la supervisión especializada donde se permite realizar un seguimiento de los riesgos de liquidez y solvencia que poseen las entidades del sector financiero, con ello permite generar confianza a los socios y clientes manteniendo un sistema regulado, sólido y estable (Superintendencia de Bancos y Seguros del Ecuador, 2017)

El reflejo de la gestión realizada por las cooperativas de ahorro y crédito es presentado y medido a través de la información reportada en estados financieros e indicadores a la Superintendencia de Economía Popular y Solidaria (Illescas, 2013)

Las captaciones en el Ecuador constituyen el negocio principal de las Entidades Financieras, mientras más se capte, mayor es la posibilidad de dar créditos, mejorar la liquidez. La salud financiera del país se mide por la buena liquidez del Sistema Bancario. El estado reconoce el Sistema Cooperativo como un medio para facilitar mejores condiciones de vida para los ecuatorianos, en el marco de los principios universales del cooperativismo, garantizando su organización respetando su naturaleza de sociedades de personas, procurando garantizar la sostenibilidad de las instituciones y la seguridad de los depósitos a sus socios.

La Superintendencia de Bancos y la Superintendencia de Economía Popular y Solidaria garantizan y regulan el funcionamiento de las intituciones financieras de los sectores públicos, privados (Tirado, 2014)

En el segmento 1 están 31 cooperativas que tienen $9´774.544,154 en activos con corte al 31 de enero del 2019 (SEPS, 2019) (anexo 1).

Geográficamente la concentración de las cooperativas de ahorro y crédito se centra en la región sierra centro (Tungurahua, Bolívar, Cotopaxi y Chimborazo), seguidas por Zamora, Azuay y Pastaza con más de 7 cooperativas por cada cien mil habitantes. El rol del sistema cooperativista es importante para el desarrollo de la micro finanza, moviliza recursos financieros tanto en las zonas rurales como urbanas marginales del país que no tienen acceso al crédito bancario (Mera Gómez, 2015)

La Superintendencia de Economía Popular y Solidaria a través de sus reglamentos y disposiciones exige llevar un control adecuado de los recursos monetarios de las instituciones financieras, además las entidades financieras deben tener una Unidad de Riesgos que se enfoque principalmente en controlar el riesgo de liquidez y solvencia, para salvaguardar el financiamiento de la entidad.

De acuerdo al análisis realizado por Herrera, Mario (2018), considera que, desde la acepción constitucional, el sistema económico popular y solidario viene a ser el conjunto de *"formas de organización económica"*, que reconocen al ser humano como sujeto y fin en la economía, y que propenden a una relación dinámica y equilibrada entre sociedad, Estado y mercado, cuyo objetivo es garantizar la producción y reproducción de las condiciones materiales e inmateriales que posibiliten el buen vivir. Allí la importancia del sector, cuyos fines responden socialmente.

El Código Orgánico Monetario y Financiero, entra en vigencia en el año 2014, cuyo objeto es "regular los sistemas monetario y financiero, así como los regímenes de valores y seguros del Ecuador" (Código Orgánico Monetario y Financiero, 2014), (Herrera, 2014)

El sector financiero público tiene como objetivo la prestación de servicios financieros de forma

sustentable, eficiente, accesible y equitativa, orientados preferentemente al incremento de la productividad y competitividad de los sectores productivos. Por su parte, el sector financiero privado está constituido por entidades que captan recursos del público para otorgar créditos y ofrecer otros servicios financieros (Cordero, 2016)

En referencia a la Tecnología y con la finalidad de prevenir riesgos asociados la Superintendencia de Bancos y Seguros en su momento determinó ciertas políticas y procedimientos que protejan los intereses financieros, planes de contingencias y continuidad que como actores principales la tienen. Bajo este contexto la Superintendencia de Bancos y Seguros promueve las "Normas generales para la aplicación de la ley general de instituciones del sistema financiero", en la que en la Sección II. Factores de Riesgo Operativo, el objetivo es minimizar las pérdidas financieras y por ende reducir el riesgo operativo, por lo deben ser adecuadamente administrados los siguientes aspectos: procesos, personas, tecnología de la información y eventos externos (Superintendencia de Bancos y Seguros, 2005).

En la normativa mencionada, las instituciones financieras en relación con el manejo de riesgo de la tecnología de información en la sección II, Art. 4, literal 4.3. define "Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones. Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información" (p.254).

Es ahí donde radica la importancia de proponer un modelo de evaluación de la gestión de Tecnología de Información basado en los marcos referenciales COBIT 5, ITIL V3, ISO 27002 y su efecto en la competitividad de las cooperativas de ahorro y crédito del segmento 1, como aporte al Gobierno de Tecnología de Información, el cual debe ser aplicado a las cooperativas de Ahorro y Crédito del Segmento 1 según nueva segmentación proporcionada por la (SEPS, 2019).

Por otro lado la experiencia en las auditorías realizadas a las áreas de Tecnología de Información de varias cooperativas del segmento 1, se basan en marcos referenciales separados, unos aplican COBIT, otros aplican ISO, ITIL, entre otras buenas prácticas, de esta manera es importante destacar que al desarrollar un marco de evaluación nuevo que englobe en un solo modelo una evaluación y auditoría integral obtengamos mejores resultados, mejore la competitividad institucional y nivel de respuesta de la gestión de Tecnología de Información en cada una de las cooperativas.

Cabe destacar que el afán de cumplir con las normativas y entes regulatorios, las cooperativas de ahorro y crédito realizan esfuerzos aislados y medianamente integrados por guiarse en marcos de referencia y buenas prácticas de gobierno de Tecnología de Información, esto justifica promover el desarrollo de un marco de referencia COBIT 5, ITIL V3, ISO 27002 y garantizar que las instituciones obtengan un modelo de madurez que les permita obtener mejores resultados basados en indicadores de gestión competitividad, implementación de nuevos procesos de gestión y asegurar la calidad de sus servicios de Tecnología de Información de manera segura y controlada.

Dicha investigación incentivará a las instituciones del sector cooperativo incorporen en sus actividades buenas prácticas de gobernanza y control asegurando la gestión de TI, investigación que puede ser aplicada en cooperativas de ahorro y crédito, entidades

financieras reguladas y deja al investigador incorporar este modelo en otras instituciones cooperativas, con el objetivo que la gestión de Tecnología de Información obtenga un alto estándar de servicios y competitividad, por otra parte genera un manejo y control de procesos adecuado minimizando riesgos asociados.

Con base a la contextualización planteada esta investigación tiene como finalidad diseñar los indicadores de la gestión y evaluación de Tecnología de Información a partir de la integración y selección de los procesos de los marcos de referencia COBIT 5, ITIL v3 e ISO 27002 en las áreas de Tecnología de Información de las cooperativas de ahorro y crédito, apoyados en las políticas del Gobierno de Tecnología de Información.

MARCO TEÓRICO

Considerando que es una investigación que se realiza en las Cooperativas de Ahorro y Crédito y que el tema se enmarca dentro de las tecnologías de información (TI), es pertinente desarrollar este marco teórico bajos los contextos de evaluación o auditoria informática, dentro del contexto de riesgos y posteriormente fundarla con los marcos de referencia de COBIT 5, ITIL v3, ISO 27002.

La Auditoría Informática es el conjunto de técnicas, procedimientos para evaluar y controlar un sistema informático, cuyo fin es validar si sus actividades son correctas y están enmarcadas dentro de los lineamientos establecidos en una Organización (Hernandez, 2017)

La Auditoría Informática realiza la evaluación de todos los procedimientos, sus entradas, procedimientos, controles, archivos, seguridad y obtención de información, además de los equipos de cómputo, debido a que proporciona los controles necesarios para que los sistemas sean confiables, garanticen la seguridad de los activos de información, aseguren la eficacia de los procesos (Pinilla Forero, 2016)

El rol fundamental de la Auditoría Interna es proveer un aseguramiento razonable sobre la efectividad de las actividades de la gestión de riesgos corporativa, verificar si los riesgos claves del negocio se gestionan apropiadamente y validar que la función del control interno sea efectiva. A Auditoría Interna no le compete efectuar:

- Establecer el apetito de riesgo.
- Imponer procesos de gestión de riesgo.
- Manejar el aseguramiento sobre los riesgos.
- Tomar decisiones en respuesta a los riesgos.
- Implementar respuestas a riesgos a favor de la administración.
- Tener responsabilidad de la gestión de riesgo (Piattini velthuis, 2014)

En los últimos años, ha sido cada vez más evidente la necesidad de un marco referencial para el control de tecnología de información. La administración debe decidir cuál es la inversión razonable en el control en Tecnología de Información y cómo lograr un balance entre riesgos e inversiones en control en un ambiente de Tecnología de Información frecuentemente impredecible. Los controles en los sistemas de información ayudan a administrar los riesgos, no los eliminan. Adicionalmente, el exacto nivel de riesgo nunca puede ser conocido ya que siempre existe un grado de incertidumbre (Derrien, 2015)

Finalmente, la Administración debe decidir el nivel de riesgo que está dispuesta a aceptar o juzgar cual puede ser el nivel tolerable, particularmente cuando se tiene en cuenta el costo, puede ser una decisión difícil para la administración. Por esta razón, la administración necesita un marco de referencia de las prácticas generalmente aceptadas de control de Tecnología de Información para compararlos contra el ambiente de Tecnología de Información existente y planificado. Existe una creciente necesidad entre los usuarios de los servicios de Tecnología de Información, de estar protegidos a través de la acreditación y la auditoría de servicios de Tecnología de Información proporcionados internamente o por

terceras partes, que aseguren la existencia de controles y seguridades adecuadas (Echenique Garcia, 2016)

En la actualidad existen diferentes estándares y guiones de buenas prácticas de Tecnología de Información que pueden ayudar a las empresas a mejorar tanto su eficacia como su eficiencia. Dichas buenas prácticas cubren todo lo relacionado con la organización, desde la gestión del ciclo de vida de los procesos, hasta el gobierno de la propia organización (Derrien, 2015)

La auditoría basada en riesgos depende del nivel de desarrollo que la propia institución del sistema financiero ha alcanzado en la gestión de riesgos en el área objeto de examen, y el grado en que han sido definidos objetivos determinados por la gerencia contra los cuales pueden medirse los riesgos asociados. Cuando la institución del sistema financiero cuenta con un sistema de gestión del riesgo adecuado en las área bajo examen, sin perjuicio de la necesidad de verificaciones adicionales propias del debido cuidado profesional, la auditoría basada en riesgos puede confiar en mayor grado en la evaluación del riesgo que la propia institución ha realizado, y desarrollar un plan basado en riesgos que complemente las acciones realizadas por la entidad y aumente el valor de las actividades de la auditoría interna (Hernández,2017)

Cuando la institución del sistema financiero cuenta con un sistema de gestión de riesgos menos desarrollado, la auditoría basada en riesgos requiere descansar más en la evaluación del riesgo que hace la propia auditoría." De ésta forma, todas las entidades financieras controladas por la Superintendencia de Bancos deberán efectuar sus revisiones de auditoría interna sobre un enfoque basado en riesgos.

COBIT

COBIT, fue lanzado en 1996, es una herramienta de gobierno de Tecnología de Información que ha cambiado la forma en que trabajan los profesionales de Tecnología de Información. COBIT vincula la tecnología informática y prácticas de control, consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores. El marco de trabajo COBIT se aplica a todos los sistemas de información, está basado en la filosofía de que los recursos de Tecnología de Información necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos. La misión de COBIT es investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores (ISACA , 2012).

Los usuarios del sistema COBIT son: La Gerencia: para apoyar sus decisiones de inversión en Tecnología de Información y control sobre el rendimiento de las mismas, analizar el costo beneficio del control. Los Usuarios Finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente. Los Auditores: para soportar sus opiniones sobre los controles de los proyectos de Tecnología de Información, su impacto en la organización y determinar el control mínimo requerido. Los Responsables de Tecnología de Información: para identificar los controles que requieren en sus áreas (ICONTEC, 2006)

El estándar tiene las siguientes características: Orientado al negocio Alineado con estándares y regulaciones "de facto" Basado en una revisión crítica y analítica de las tareas y actividades en Tecnología de Información Alineado con estándares de control y auditoría (COSO ERM II, IFAC, IIA, ISACA, AICPA) La estructura conceptual se puede enfocar desde tres puntos de vista:

a. Los criterios empresariales que deben satisfacer la información

b. Los recursos de las Tecnología de Información
c. Los procesos de Tecnología de Información (Baud, 2016).

En COBIT se establecen los siguientes recursos en Tecnología de Información necesarios para alcanzar los objetivos de negocio: Aplicaciones: Incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información. Información: Son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio. Infraestructura: es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones. Personas: son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran (Figueroa Morán , Paladines Morán, & Caicedo Plúa, 2017).

La estructura de COBIT se define a partir de una premisa simple y pragmática: "Los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos". COBIT se divide en tres niveles:

1. ***Dominios:*** Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
2. ***Procesos:*** Conjuntos o series de actividades unidas con delimitación o cortes de control.
3. ***Actividades:*** Acciones requeridas para lograr un resultado medible. La siguiente figura muestra la relación entre procesos de Tecnología de Información (ISACA , 2012), Criterios de información y recursos requeridos:

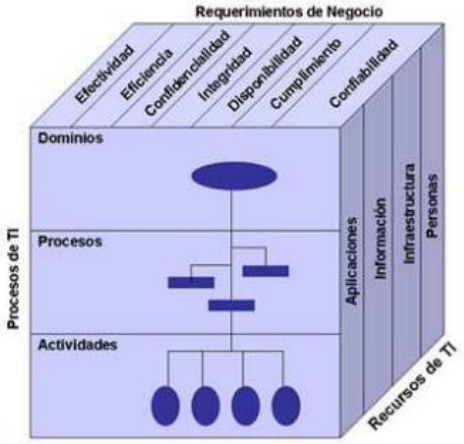


Gráfico 2. Criterios de información y recursos
Fuente: (ISACA , 2012)

ITIL

En este punto se incluirá una descripción general sobre Information Technology Infrastructure Library más conocido por su abreviatura ITIL. Además, se incluirá un breve resumen sobre cada uno de los cinco libros que forman la tercera versión de ITIL. ITIL es una guía de buenas prácticas para la gestión de servicios de Tecnologías de Información (TI) que fue creada en su primera versión en la década de 1980. A pesar de su fecha de desarrollo, no fue adoptada hasta mediados de la década de 1990 (Fonseca Luna, 2011).

En su primera versión ITIL estaba formado por un total de 10 libros principales más una serie de libros complementarios que trataban sobre temas relacionados. Tras esta primera versión, se creó una segunda versión que recogía toda la información anterior mediante una gran reestructuración en dos libros importantes más cinco libros complementarios.

Por último en el año 2007 se creó la tercera versión de ITIL formada por cinco libros: Estrategia de servicios, Diseño de servicios, Transición de servicios, Operación de servicios y Mejora Continua de servicios, que serán explicados de forma individual más adelante (Muñoz Razo, 2014). A continuación, se

muestra una imagen en la cual se puede observar la estructuración en torno al ciclo de vida que realiza ITIL en la creación de servicios:

Gráfico 3. Ciclo de vida de ITIL
Fuente: (Cansado Valle, 2018)

A pesar de tratarse de una guía de buenas prácticas de Tecnología de Información, ITIL no dispone de certificaciones para las empresas. Las certificaciones de ITIL se pueden obtener de manera individual. Por lo tanto si una empresa desea obtener un reconocimiento dentro de ITIL la mejor opción es disponer en su plantilla de personal que se encuentre certificado de forma individual (Solares Soto , Baca Urbina, & Acosta Gonzaga, 2014). Las posibles certificaciones que se pueden obtener de ITIL son las siguientes:

- **ITIL Foundation:** Esto quiere decir que se dispone del conocimiento general sobre los elementos clave del ciclo de vida de ITIL.
- **ITIL Intermediate:** Esto quiere decir que se dispone del conocimiento y las competencias necesarias para la gestión de áreas específicas basadas en las buenas prácticas que propone ITIL
- **ITIL Expert:** que disponen de las certificaciones anteriores y desean demostrar un conocimiento superior acerca de todo el contenido de ITIL.
- **ITIL Master:** Es la máxima certificación que se puede obtener dentro de ITIL (Solares Soto , Baca Urbina, & Acosta Gonzaga, 2014).

ITIL v3 Estrategia del Servicio

Representa la parte entorno la cual gira el ciclo de vida. La estrategia de servicio permite definir objetivos y estrategias de cara al cliente y al mercado, a la vez que ayuda a identificar y seleccionar las oportunidades para la compañía. Por todo esto, se define como la parte central sobre la que gira el ciclo de vida. Las actividades más importantes para la creación de una correcta Estrategia de Servicio como son: definición del mercado, desarrollo de ofertas, desarrollo de los activos estratégicos y preparación de la implementación. Cuenta con tres procesos importantes a nivel estratégico:

- Gestión Financiera.
- Gestión de la Demanda.
- Gestión de la Cartera de Servicios (Baud, 2016)

ITIL v3 Diseño del Servicio

Es la segunda fase dentro del ciclo de vida, es la fase posterior a la Estrategia del Servicio. El objetivo principal es realizar el diseño de servicios nuevos o modificados para su posterior desarrollo y paso a producción. Además, uno de los aspectos principales de la fase de diseño es obtener la máxima calidad en los servicios (Machado & Torres, 2016). Los cinco aspectos más importantes dentro del diseño son los siguientes:

- Solución del servicio.
- Cartera de servicios.
- Diseño de procesos.
- Diseño de métricas y sistemas de medición (OGC, 2011).

Además, de lo mencionado anteriormente existen siete procesos de la fase de diseño:

- Gestión del Catálogo de Servicios. – Gestión del Nivel de Servicio.
- Gestión de la Capacidad.
- Gestión de la Disponibilidad.
- Gestión de la Continuidad del Servicio de TI.
- Gestión de la Seguridad de la Información.
- Gestión de Proveedores (OGC, 2011)

ITIL v3 Transición del Servicio

Explica cómo convertir las especificaciones del diseño en un servicio nuevo o en la modificación de un servicio existente. El objetivo principal de esta fase consiste en la coordinación de los procesos, sistemas y funciones necesarios para la construcción, prueba y despliegue de una versión de un determinado servicio en el entorno de producción (Zea & Beatriz, 2015). Los pasos más importantes dentro de la Transición del servicio son los siguientes:

- Planificación y preparación
- Construcción y pruebas – Versiones piloto.
- Planificación y preparación del despliegue del servicio.
- Despliegue y transición.
- Revisión y cierre de la fase de Transición del Servicio (Bon, Jong, Axel, & Mike, 2014)

Dentro de la Transición del Servicio existen una serie de procesos y actividades que se explican y definen a lo largo del documento referido. Los procesos y actividades son los siguientes:

- Planificación y soporte a la Transición
- Gestión de Cambios
- Gestión de la Configuración y Activos del Servicio.
- Gestión de Versiones y Despliegues
- Validación y pruebas del Servicio
- Evaluación
- Gestión del Conocimiento del Servicio (Cely-Sánchez, 2015)

ITIL v3 Operación del Servicio

Explica las actividades diarias que se deben seguir para el correcto funcionamiento de los diferentes servicios existentes en la compañía. El objetivo principal de esta fase consiste en realizar la coordinación y la ejecución de actividades y procesos necesarios para conseguir la entrega y la gestión de los diferentes servicios que se ofrecen a los usuarios de la empresa y a los clientes. Durante esta fase es necesario recoger datos del rendimiento diario de los servicios para observar cuando es necesario realizar alguna mejora sobre alguno de los servicios (Gutiérrez , 2017). Existen dos tipos de mejoras disponibles para la Operación del Servicio:

- Mejora incremental a largo plazo.
- Mejora continua y a corto plazo.

Los procesos y actividades en los que se basa la Operación del Servicio, y por lo tanto aparecen definidos en el libro son los siguientes:

- Gestión de Eventos
- Gestión de Incidencias
- Gestión de Peticiones
- Gestión de Problemas
- Gestión de Accesos
- Monitorización y control
- Operaciones de Tecnología de Información (Gutiérrez , 2017)

ITIL v3 Mejora Continua del Servicio

Explican las actividades que son necesarias realizar para adaptar los servicios a las nuevas necesidades. Esto quiere decir que es necesario ir identificando e implementando mejoras de los diferentes servicios de forma continua durante todo el tiempo que el servicio este en uso. El principal objetivo de esta fase del ciclo de vida consiste en obtener una mejora continua de la eficacia y la eficiencia de los servicios para poder alcanzar los objetivos de la compañía (Gutiérrez , 2017). Para implementar la mejora continua del servicio se utiliza el ciclo de

Deming que está basado en la ejecución cíclica de las siguientes cuatro actividades:

- Planificar
- Hacer
- Verificar y,
- Actuar

Para realizar una medición de la mejora continua se utilizan las siguientes tres métricas:

- Métricas de tecnología que miden el rendimiento y la disponibilidad de las aplicaciones.
- Métricas de proceso que miden el rendimiento de los procesos.
- Métricas de servicio que disponen de los resultados del servicio final (Baud, 2016)

ISO 20000

En este punto se incluirá una descripción general sobre ISO/IEC 20000 – Service Management. ISO 20000 es una normativa publicada en 2005 por las siguientes organizaciones internacionales: International Organization for Standardization (ISO) e International Electrotechnical Commission (IEC). ISO 20000 proviene de la serie BS 15000 creada por British Standarsds Institution (BSI) (Morán Abad & Pérez Sánchez, 2016)

ISO 27002

ISO 27002 consiste en una guía de buenas prácticas que permiten a las organizaciones mejorar la seguridad de su información. Con este fin, define una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones.

Éstos se hallan distribuidos en diferentes dominios que abarcan de una forma integral todos los aspectos que han de ser tenidos en cuenta por las organizaciones.

Dominios de la ISO 27002

Estos dominios que estructura la ISO 27002 son:

1. La política de seguridad.
2. Los aspectos organizativos de la seguridad de la información.
3. La gestión de activos.
4. La seguridad ligada a los recursos humanos.
5. La seguridad física y ambiental.
6. La gestión de las comunicaciones y de las operaciones.
7. Los controles de acceso a la información.
8. La adquisición, desarrollo y mantenimiento de los sistemas de información.
9. La gestión de incidentes en la seguridad de la información.
10. La gestión de la continuidad del negocio.
11. Los aspectos de cumplimiento legal y normativo.

Se debe señalar que la única norma a certificar de la serie es la ISO 27001. No así la ISO 27002, que, como hemos comentado, tan sólo establece una serie de recomendaciones y buenas prácticas.

También hay que tener presente que para lograr la certificación en ISO 27001 no es necesario implantar todos los controles recomendados por la ISO 27002, sino que la organización debe priorizar y seleccionar aquellos controles que se alineen con su estrategia de riesgo, teniendo en cuenta la capacidad presupuestaria de la organización y sus necesidades de negocio (Bejunmea, 2018)

METODOLOGÍA

En las Cooperativas de Ahorro y Crédito, el plan de contingencia, la disponiblidad y continuidad del negocio, así como también el riesgo operativo, son componentes críticos de la estrategia de estas organizaciones, por esta razón para la metodología de apoyo se identifica politicas, normas , procedimientos y estándares que se alinean a las necesidades de cada cooperativa de estudio, basados en recomendaciones y buenas prácticas de Tecnología de Información. Bajo estas premisas la metodología que se utilizó fue aplicativa, cualitativa, explorativa, bibliográfica y de caso de estudio.

Aplicativa, ya que busca evidenciar la problemática de estudio, en base a la aplicación de los conocimientos, con la finalidad de a través de las debilidades identificadas se establezca recomendaciones para la optimización de recursos. Mejorando la productividad y satisfacción de los usuarios.

El enfoque cualitativo, porque permite realizar una descripción detallada de cada uno de los procesos de las COACs e identifcar la necesidad de la incorporación de buenas prácticas de Tecnología de Información.

El tipo de investigación es descriptiva con corte transversal, ya que permite realizar una descripción detallada de cada uno de los procesos de las COACs es identifcar la necesidad de la incorporación de buenas prácticas de Tecnología de Información, que coadyuve al mejoramiento de su gestión de servicios y minimizar el riesgo. Mientras que, la explorativa abordaremos todo el escenario de estudio a través de la obtención de datos que conducirán a la formulación de las preguntas de investigación, apoyadas de la investigación bibliográfica que mediante técnicas y estrategias, accederemos a fuentes de consulta primarias y secundarias pertinentes para la investigación.

Para el caso de estudio se considerarán los criterios de las metodologías COBIT, ITIL e ISO, en donde se estimarán los dominios, procesos y áreas de cada uno de ellos lo que permitirá construir un solo modelo de evaluación de la gestión de Tecnología de Información para las Cooperativas de estudio.

El Proceso Metodológico que se aplicó en esta investigación se describe en el gráfico 4:

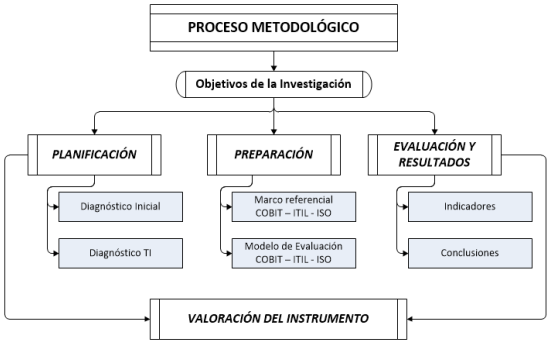


Gráfico 4. Proceso metodológico
Elaboración propia

El alcance la investigación se centra en la construcción de un modelo de evaluación de gestión de Tecnología de Información que aborde los criterios de COBIT, ITIL e ISO, aplicado a las cooperativas de ahorro y crédito integradas a la normativa y buenas practicas de la gestión de riesgo a las que se ven abocadas, con la finalidad de contar con un informe que permita a las instituciones de estudio contar con información para toma de decisiones preventivas y oportunas.

Según (Seyal, Sheung, & sharul, 2016) corresponde realizar un análisis de las escalas COBIT y determinar el grado de cumplimiento y desempeño en base a COBIT; a su vez concuerda que cada marco de referencia debe ser evaluado para luego ser integrado y direccionado a las buenas prácticas ITIL como ISO 27000.

La población de estudio lo representan las 2 Cooperativas del segmento 1, la primera con característica de gran tamaño y la segunda de tamaño mediano de la Provincia del Carchi, tomadas del ranking de COACs de la Superintendencia de Economía Popular y

Solidaria y cumpliendo con los preceptos de confidenciailidad no se considerarán sus nombres reales, sin embargo se ha colocado la identificación siguiente con una característica real categorizandose así: COAC GR y MD, respectivamente (anexo 1).

ANÁLISIS DE RESULTADOS

Al desarrollar el proceso metodológico de la investigación , se tiene:

a. Planificación

a.1. Diagnóstico Inicial

Para el diagnóstico inicial se recopiló la información de las Cooperativas de estudio, teniendo los siguientes resultados.

Dentro de las características a resaltar es la calificacion de riesgos integrales de las COACs, la GR es BBB+, mientras que la COAC MD es AA (anexo 2).

Como se observa las COACs de estudio cuentan con la información institucional que los organismos de control exigen para su normal funcionamiento, y son los que rigen el accionar de las mismas para mantener su competitividad y posicionamiento, dentro del contexto financiero.

Los mismos que al ser rervisados cuentan con la estructura básica de cada uno de los componentes institucionales.

a.2. Diagnóstico de Tecnología de la Información

La información que se consideró para el diagnóstico de Tecnología de Información en las COACs de estudio fueron: Orgánico, Plan Estratégico, POA, Manual de Políticas y Funciones del Departamento de Tecnología de Información.

En relación con el orgánico del área de Tecnología de Información de las COACs se tiene el orgánico de la COAC GR (anexo 3) y el orgánico de la COAC MD (anexo 4), El análisis del organigrama de cada COAC se lo analiza desde su tipo ahasta su composición (anexo 5).

Como se observa la estructura orgánica de mayor complejidad es la de la COAC GR con mayores áreas y mayor personal que la COAC MD, además la primera tiene una estructura horizontal vertical; mientras que, la segunda es solo vertical, en los dos casos se cuenta con manual de funciones.

Entre el Plan Estratégico y POA de Tecnología de Información , las dos cuentan con estos instrumentos necesarios para la planificación, ejecución y seguimiento de toda organización, al valorar su estructura se tiene el resultados (anexo 6):

En relación con el total de elementos analizados (8) la COAC GR alcanza un cumplimiento del 88%, mientras que la COAC MD el 63% de cumplimiento.

Por último se analiza el manual de políticas de las COACs, en base a 13 elementos (anexo 7)

En relación con los elementos del manual de políticas la COAC GR cubre el 77% y la COAC MD el 69%, además la segunda cooperativa tiene una estructura que se asemeja mucho al modelo ITIL, mientras que la primera tiene una estructura similar al modelo COBIT, los dos manuales tienen coincidencias en seis elementos: tecnología, infraestructura, seguridad, manejo del software, cambios e información.

b. Preparación

b.1. Marco referencial COBIT 5 ITIL v3 e ISO 27002

(IT GOVERNANCE INSTITUTE, 2008) propone una alineación de los marcos de referencia COBIT 4.1, ITIL V3 e ISO 27002, en pos de ayudar a las distintas empresas a obtener un marco estándar en donde el negocio debe priorizar y sea una soporte competitivo para la toma de decisiones en la alta gerencia.

Para analizar el marco referencial de COBIT 5. ITL v3 e ISO 27002, se partió de la revisión bibliográfica y documental existe para establecer un análisis comparativo de las tres

metodologías que se pretenden enlazar para establecer el modelo de evaluación de gestión de riesgo, como se muestra en la tabla 3.

Tabla 2. Análisis comparativo del marco de referencia

COMPONENTES / MODELO	COBIT	ITIL	ISO
FUNCIONES	Mapeo de Procesos IT	Mapeo de La Gestión de Niveles de Servicio de Ti	Marco de Referencia de Seguridad de la Información
ÁREAS	5 Dominios 37 Procesos	5 Procesos 29 Áreas	7 Dominios 14 objetivos
CREADOR	ISACA	OGC	ISO International Organization For Standardization
FUNCIÓN	Auditoría de Sistemas de Información	Gestión de Niveles de Servicio	Cumplimiento del estándar de seguridad

Elaboración propia

Posteriormente se estructura una matriz relacional de datos cruzados, en relación con los tres modelos y los componentes de cada uno (anexo 8), con a finaidad de estaber la relación entre los 3 modelos de estudio.

En el anexo 9 se establece una matriz en la que se coloca los componentes que se interrelacionaron en paso anterior, y se establecen interrogantes que erán los ítem guías de la evaluación por cada dominio del modelo propuesto y según las necesidades de las COACs del segmento 1.

b.2. Modelo de Evaluación de la Gestión de Tecnología de Información bajo COBIT 5-ITIL V3-ISO 27002

En base a la matriz relacional se determina que el modelo que se establecerá como base será COBIT bajo sus cinco procesos: EDM – APO – BAI – DSS – MEA, y estos serán relacionados con las áreas y dominios de ITL 5 e ISO 27002, respectivamente, así como también se establecerá las preguntas bajo el cual se estructura el modelo de evaluación de gestión de Tecnología de Información, esta inhibrigación (anexo 10), para el que se aplicará los siguientes criterios de evaluación incorporado el método de semaforización, en el cual el color rojo señala que el riesgo es alto; tomate oscuro, tomate claro y amarillo corresponden a riesgo medio; amarillo y amarillo claro se asignan como riesgo bajo; y, el verde no existe riesgo, como se muestra en la tabla 7:

Tabla 3. Criterios del modelo de evaluación

CRITERIOS DE EVALUACIÓN	
No realizado	0%
Realizado informalmente	20%
Planificado	40%
Bien definido	60%
Cuantitativamente controlado	80%
Mejora continua	100%

Elaboración propia

Otro componente que se considero importante es el planteamiento de

Indicadores para cada dominio del modelo de evaluacion propuesto, tal es asi que se tienen los siguientes indicadores, como se muestra en la tabla 5:

Tabla 4. Indicadores

INDICADOR	FÓRMULA
Nivel Organizacional	N° de personas en áreas de TI que producen beneficio directo a la COAC / N° Total de personas que laboran en el área de TI
Nivel de soluciones técnológicas	N° de soluciones tecnológicas que no están alineadas con la estrategia de la COAC / Cantidad de requerimientos tecnológicos requeridos para la estrategia de la COAC
Nivel de cambios, capacidad y funcionalidad	Total de cambios, instalaciones, configuraciones realizados (mensual) / N° de cambios, instalaciones, configuraciones fallidas (mensual)
Nivel de mantenimiento	N° de equipos que han recibido mantenimiento (anual) / Total de equipos (anual)
Elaboración de software propio	N° de software realizados por el equipo de TI (anual)
Nivel de incidencias	Cantidad de incidencias resueltas de sistemas caídos por capacidad o desempeño de procesamiento insuficiente (mensual) / Total de incidencias denunciadas de sistemas caídos por capacidad o desempeño de procesamiento insuficiente (mensual)
Nivel de vulnerabilidad	N°. De vulnerabilidades reportadas / N°. De vulnerabilidades cubiertas
Nivel de auditoría	N°. De auditorías realizadas en el año
Nivel de calidad	N° de sistemas auditados / Total de sistemas existentes en la COAC

Elaboración propia

Con base al análisis desarrollado se cuenta con el instrumento de evaluación de gestión de TI según COBIT 5 – ITIL V3 e ISO 27002 (anexo 11). Una vez establecido el modelo se lo aplicó a las dos COACs de estudio, en el cual se reflejan los siguientes resultados en la tabla 6:

c. Evaluación y Resultados e Indicadores

Tabla 5. Resultados Diagnósticos

	% DE CUMPLIMIENTO		
DOMINIO	COAC GR (B-)	COAC MD (AA)	VALOR ESPERADO (/100%)
Evaluar, Orientar y Supervisar (EDM)	60.0	64.0	100
Alinear, Planear y Organizar (APO)	65.6	63.6	100
Construir, Adquirir e Implementar (BAI)	60.0	67.1	100
Entregar, Dar Servicio y Soporte (DSS)	52.0	58.3	100
Supervisar, Evaluar y Valorar (MEA)	60.0	45.0	100
PROMEDIO	59.5	59.6	
	RIESGO PLANIFICADO		

Elaboración propia

Las COACs de estudio al aplicar el modelo de evaluación de gestión de Tecnología de Información propuesto, refleja que su gestión se encuentra en un riesgo planificado, lo que significa “Los controles de seguridad de la información establecidos son planificados, implementados y repetibles”, siendo la debilidad en la cooperativa grande el dominio “Entregar, Dar servicio y soporte (DSS)”, en el item de protección de gestión de vulnerabilidad técnica y gestión integral de seguridad. Mientras que en la cooperativa mediana en el mismo dominio de la COAC GR y en los mismos ítems, además el dominio de “Supervisar, Evaluar y Valorar (MEA)”, en los íems de: auditorías pues estas se realizan solo manualmente no existe un sistema informático para esta gestión, supervisión de uso de sistemas y protección de la información de los registros.
Gráficamente se muestra los resultados del modelo a través de un gráfico de red:

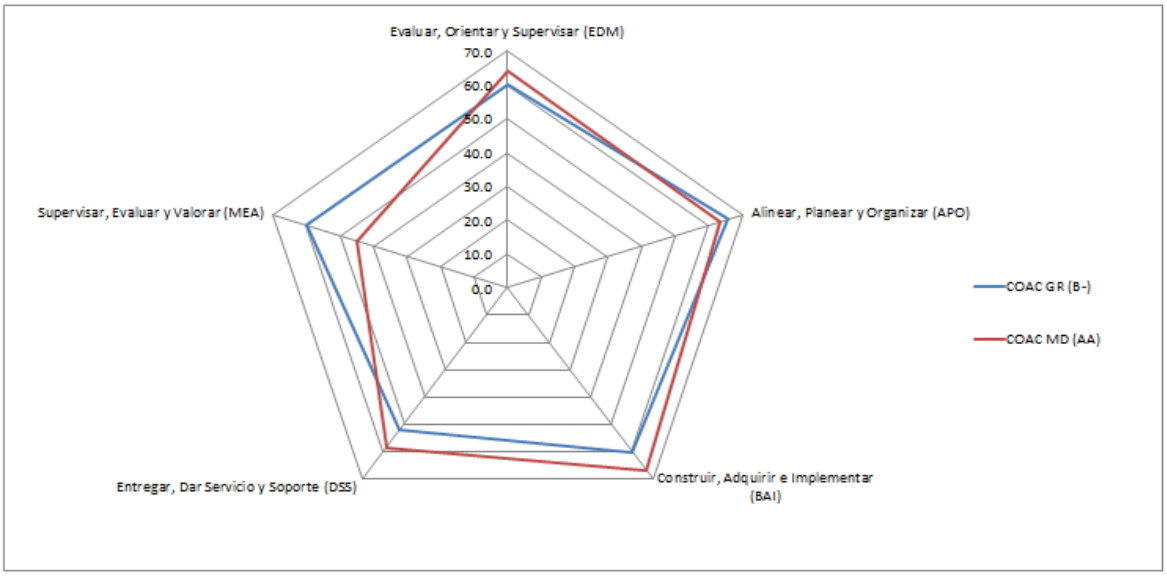


Gráfico 5. Resultados comparativos de evaluación
Elaboración propia

En relación con el análisis sobre la base a los indicadores antes descritos en la tabla 7 se tiene la siguiente relación, en la COACs de estudio:

Tabla 6. Análisis de Indicadores de las COACs de estudio

	INDICADORES	
DOMINIO	**COAC GR (B-)**	**COAC MD (AA)**
Nivel Organizacional	75%	65%
Nivel de soluciones técnológicas	3%	3%
Nivel de cambios, capacidad y funcionalidad	70%	10%
Nivel de mantenimiento	95%	85%
Nivel de elaboración de software	50%	20%
Nivel de incidencias	65%	40%
Nivel de Seguridad	65%	65%
Nivel de auditoria	60%	25%
Nivel de calidad	50%	40%
PROMEDIO	**59%**	**39%**
	RIESGO BIEN DEFINIDO	**RIESGO INFORMAL**

Elaboración propia

Se destaca que las COAC GR tiene riesgo bien definido, lo que significa “Los controles de seguridad de la información además de planificados son documentados, aprobados e implementados en toda la organización” reflejándose como debilidad: nivel de soluciones tecnológicas, de elaboración de software y de calidad.

Mientras que en la COAC MD refleja un nivel de riesgo categorizado como informal “Existen procedimientos para llevar a cabo ciertas acciones en determinado momento. Estas prácticas no se adoptaron formalmente y/o no se les hizo seguimiento y/o no se informaron adecuadamente”, sobre rodo en los indicadores: nivel de soluciones tecnológicas, de cambios, capacidad y funcionalidad, de elaboración de software y de seguridad.

Este análisis de indicadores también se lo demuestra de manera gráfica a manera de red:

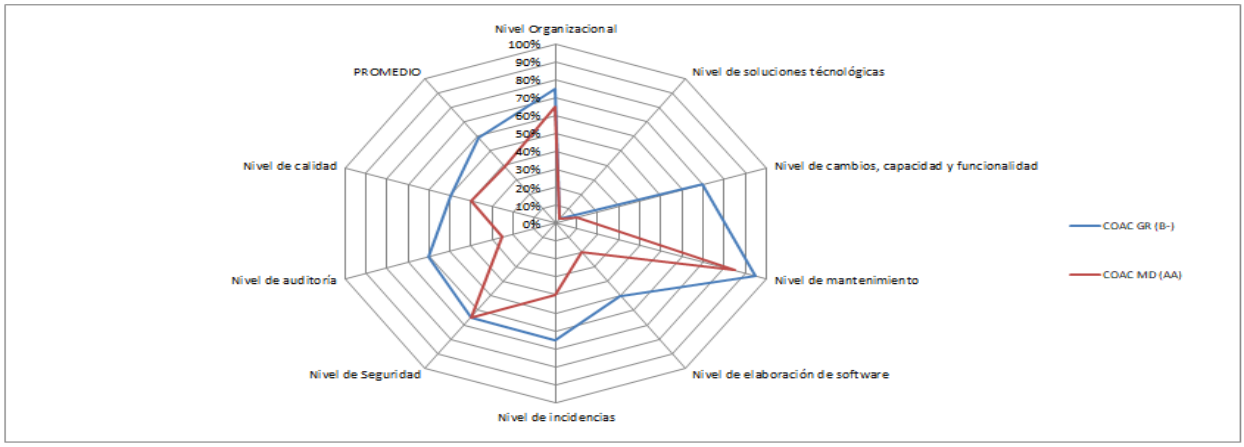


Gráfico 6. Análisis de Indicadores
Elaboración propia

d. Validación del Instrumentos

Posteriormente a la aplicación del modelo diagnóstico propuesto en las cooperativas de estudio COAC GR y COAC MD, se procede a la validación del instrumento al aplicarlo en tres cooperativas de similares

características, en tamaño y que correspondan al segmento 1, considerando si todos los elementos planteados en el modelo se acoplan y/o correlacionan con otro tipo de instituciones del mismo contexto, para este caso se aplicó en las COACs “A” , “B” y “C”, no se considerará los nombres por elementos de confidencialidad.

Donde se demostró que el modelo diagnóstico propuesto bajo COBIT 5, ITIL V3 e ISO 27002, es válido para otro tipo de cooperativas, ya que arroja resultados capaces de tomar decisiones a nivel directivo, como se muestra en la tabla 8 y gráfico 7:

Tabla 7. Validación del Instrumento

DOMINIO	% DE CUMPLIMIENTO			
	COAC "A" (AA-)	COAC "B" (A)	COAC "C" (A)	VALOR ESPERADO (/100%)
Evaluar, Orientar y Supervisar (EDM)	56.0	75.4	55.6	100
Alinear, Planear y Organizar (APO)	62.5	74.5	67.4	100
Construir, Adquirir e Implementar (BAI)	61.7	76.4	84.0	100
Entregar, Dar Servicio y Soporte (DSS)	45.0	43.2	47.0	100
Supervisar, Evaluar y Valorar (MEA)	57.0	30.0	30.0	100
PROMEDIO	56.4	59.9	56.8	
	RIESGO PLANIFICADO			

Elaboración propia

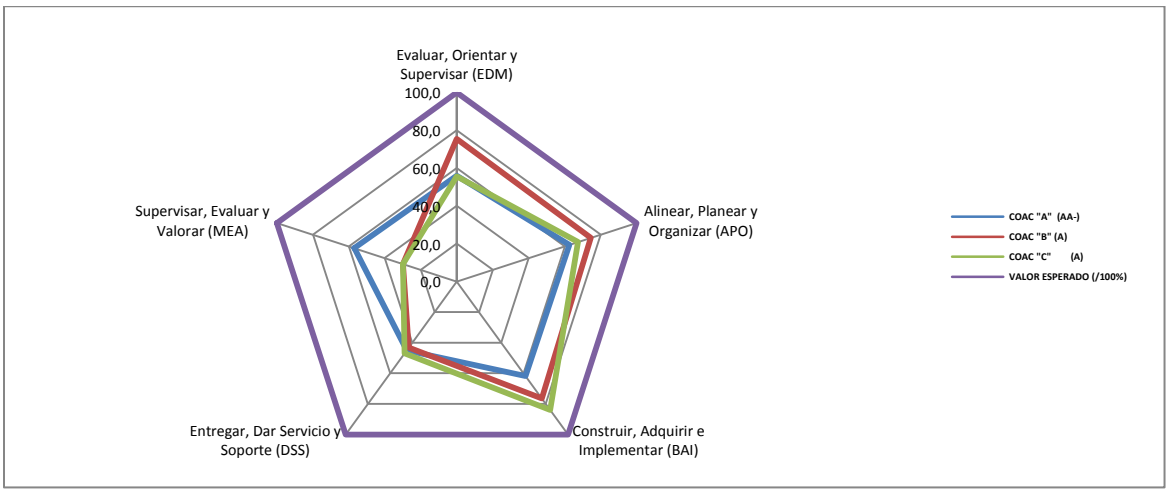


Gráfico 7. Validación del instrumento
Elaboración propia

Como se demuestra el instrumento propuesto es aplicable a todo tipo de COAC de similares características, aunque el nivel de riesgo de éstas no sea el mismo. En esta validación se demuestra que la gestión del área de Tecnología de Información de las tres COACs se encuentra encuentran en un nivel de riesgo planificado (Los controles de seguridad de la información establecidos son planificados, implementados y repetibles), y los dominios que requieren mayor atención, por no estar bien definida su

gestión son : EDM en las COACs “A” y “C”, las tres COACs en el dominio DSS, y en el dominio MEA sobre todo las COACs “B” y “C”. sobre todo en la supervisión del uso de los sistemas y la protección de la información de los registros, por lo que es donde se sugiere al nivel directivo tomar acciones correctivas. En relación con los indicadores del modelo de evaluación propuesto se tienen los siguientes resultados:A pesar de que el modelo de evaluación de la gestión de Tecnología de Información, arrojo las primeras debilidades, al aplicar la matriz de indicadores, resaltan inconsistencias mucho más precisas pára toma de decisiones:

Tabla 8: Matriz de Indicadores

	INDICADORES		
DOMINIO	**COAC "A" (AA-)**	**COAC "B" (A)**	**COAC "C" (A)**
Nivel Organizacional	80%	85%	80%
Nivel de soluciones técnológicas	10%	3%	8%
Nivel de cambios, capacidad y funcionalidad	7%	17%	13%
Nivel de mantenimiento	60%	85%	75%
Nivel de elaboración de software	50%	55%	60%
Nivel de incidencias	45%	55%	50%
Nivel de Seguridad	70%	85%	75%
Nivel de auditoría	50%	25%	30%
Nivel de calidad	50%	30%	25%
PROMEDIO	**47%**	**49%**	**46%**

Elaboración propia

Coincide que la mayor debilidad es el nivel de soluciones tecnológicas, de cambios, capacidad y funcionalidad y el de auditoría.

Conclusiones

La propuesta planteada se armoniza los criterios técnicos de COBIT 5, ITIL V3 e ISO 27002, tomando como base a la primera metodología, consolidando con las necesidades de las COACs de estudio, asi como con los condicionantes de riesgo financiero.

Al análisis se inicia desde el componente organizacional en donde se destaca que la COAC Grande se encuentra bajo una estructura COBIT 5 y la COAC Mediana bajo ITIL v3.

El modelo de evaluación de gestión de Tecnología de Información propuesto busca conocer el gobierno y gestión de Tecnología de Información, observar el impacto de los riesgos tecnológicos, valorando controles y midiendo su efectividad, en procura de minimizar la afectación sobre los activos de tecnología.

La aplicación de la herramienta de trabajo denominada “Modelo de evaluación de gestión de Tecnología de Información” junto con el marco metodológico empleado para esta evaluación tecnológica han revelado que COAC grande valora su gestión de Tecnología de Información como riesgo moderado; mientras que la mediana como tiene un nivel como riesgo definido.

Se pudo determinar que el gobierno y gestión de tecnología de información de las COACs de estudio, según los resultados del modelo de diagnóstico propuesto, se alinea a marcos de referencia y buenas prácticas, puntualmente COBIT 5 como eje del modelo con alineamientos de ITIL e ISO 27002.

Dentro de los principales hallazgos a la aplicación del modelo de Diagnóstico de gestión de Tecnología de Información se tiene:
No todas las COACs tienen definida un área de auditoría informática, única que tiene es la COAC GR y la COAC “A”;
Las COACs no tienen definido un marco de referencia integral, cada COAC tiene una orientación metodológica derfinida y hasta el momento no se ha estandarizdo, por lo que es necesario que todas las COACs se alineen a los tres marcos de referencia COBIT 5, ITIL v3 e ISO, incluidas seguridades;
Ninguna de las COACs esta certificada a ISO y las COACs de estudio y de validación estan llegando a un promedio de madurez en la gestión de Tecnología de Información en un 58,44%, encontrándose mejor ubicadas la COAC GR y la B.

Otro elemento que se consideró dentro de la evaluación es la aplicación de indicadores, armonizados con los dominios, objetivos de las metodologías así como las necesidades de las COAC, el indicador de mayor debilidad es el de nivel de soluciones tecnológicas, nivel de cambios, capacidad y funcionalidad, así como nivel de auditoría y calidad, en virtud de que estas ultimas no se apoyan en herramientas tecnológicas, sino manuales y empiricas.

El modelo de evaluación de gestión de Tecnologías de Infromación, se demuestra que es aplicable a todas las COAC que tienen condiciones similares.

Las cooperativas no implementan buenas practicas de gobierno, ya que en sus planes operativos y planes de TI, no contemplan normativas externas, se centran en las politicas y controles de la SEPS.

No contemplan en sus presupuestos de TI, mejoramiento o implementaciones de Gobierno de TI.

No disponen de una gestion ni sistema de indicadores de evaluacion de la gestion de TI, se rigen a disponer de una mesa de TI, soporte y mantenimiento y gestion de cambios para determinadas actividades y areas de TI.

Diponen de prácticas gestionadas por la Jefatura de Turno, no se da continuidad a la gestión de TI y uso de practicas internacionales.

Se deja para investigaciones futuras se realice una evaluación de la efectividad del modelo de evaluación propuesto, promoviendo el uso y cumplimiento de las normativas internas de las COACs, realizando una evaluación del modelo propuesto vs las normativas de los entes de control ecuatorianos.

Incoporar la adopcion del modelo de evaluacion propuesto para fortalecer la gestion de TI agregando control y valor a las instituciones de ahorro y credito del pais.

Mejorar la tecnologia en cuanto a la obsolecencia de infraestructura de TI, en razón de que los mayores porcentajes de vulnerabilidades en los servicios obedecen a la gestión de capacidad y disponibilidad.

Hacer el seguimiento a la COAC en donde se incoporara el modelo de evaluación, mediante indicadores de gestión financiera y cumplimiento de los principios de seguridad.

REFERENCIAS BIBLIOGRÁFICAS

Echenique Garcia, J. (2016). *Auditoría en informática.* Mexico: Editorial McGraw-Hill.

Código Orgánico Monetario y Financiero. (septiembre de 2014). *Segundo Suplemento -- Registro Oficial Nº 332*. Quito, Ecuador: Asamble Nacional.

Superintendencia de Bancos y Seguros del Ecuador. (12 de julio de 2017). Recuperado el 11 de MARZO de 2019, de El Sistema Financiero. En A. Pena, Reporte de Estabilidad Financiera: http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/La%20SBS/reporte_estabilidad _20

Aguasaco , W. J., & Flórez , J. A. (2017). *Diseño de un modelo de implementación de itil v3 (biblioteca de infraestructura de tecnologías de información) para el mejoramiento en los procesos del departamento de sistemas en la Fundación Santa Fe De Bogotá.* Bogotá: Fundación Santa Fe De Bogotá.

Arzbach, M. (2015). *Regulación y Supervisión de Cooperativas de Ahorro y Crédito en América Latina y el Caribe.* San José: Confederación Alemana de Cooperativas Confederação Alemã das Cooperativas., San José.

Asamblea Nacional. (2011). Ley Orgánica de la Economía Popular y Solidaría y del Sector Financiero Popular y Solidario. *Registro Oficial 444 de 10-may.-2011. Última modificación: 23-oct.-2018*. Quito, Ecuador.

AUKEN, V., Madrid Guijarro, A., & Garcia, D. (2008). Innovation and SME Performance in Spanish Manufacturing Firms.

Badía Giménez, A. (2011). *Calidad: Modelo ISO 9001 Versión 2000.* Editorial Deusto.

Baud, J. (2016). *ITIL - V3: Entender el Enfoque y Adoptar las Buenas Prácticas.* Barcelona: Eni Ediciones.

Bauset, C. (2013). *Gestión de los servicios de tecnologías de la información: modelo de aporte de valor basado en ITIL.*

Bejunmea, O. (23 de junio de 2018). *¿Sabes diferenciar la ISO 27001 y la ISO 27002?* Recuperado el 5 de abril de 2019, de http://www.redseguridad.com/especialidades-tic/certificaciones-y-formacion/sabes-diferenciar-la-iso-27001-y-la-iso-27002

Bon, J., Jong, A., Axel, K., & Mike, P. (2014). *Estrategia del Servicio Basada en ITIL V3.* LondresLondresLondresLondresLondres LondresLondres: Editorial Van Haren Publishin.

Bordas, M. (2016). GESTIÓN ESTRATÉGICA DEL CLIMA LABORAL. En M. J. MARTINEZ, *GESTIÓN ESTRATÉGICA DEL CLIMA LABORAL.*

Calidad ISO 9001. (julio de 2013). *ISO 9001 calidad. Sistemas de Gestión de Calidad según ISO 9000. Cómo elaborar un flujograma.* Recuperado el 23 de octubre de 2018, de http://iso9001calidad.com/como-elaborar-un-flujograma-136.html

Cando, P. (2019). *Revision de Misión y Visión Cooperativas Segmento 1 Ecuador.* Quito.

Cansado Valle, S. D. (2018). Estudio de la fase de Operación del Servicio de ITIL. *Proyecto Fin de Carrera. [En línea]. Disponible desde: http://bibing.us.es/proyectos/abreproy/12465/fichero/PFC-2465-CANSADO.pdf*.

Sevilla: Escuela Técnica Superior de Ingeniería.

Cely-Sánchez, A. (2015). *Instrumentación de itil V3 en la estrategia del servicio para el área de tecnología de la empresa multiproyectos DMC.* España.

Cordero, F. (2016). *Ley Orgánica de Economía Popular y Solidaria.* Quito.

Derrien, Y. (2015). *Técnicas de la auditoria informática.* Mexico: Editorial Alfaomega.

Figueroa Morán , G., Paladines Morán, J., & Caicedo Plúa, P. (2017). *Modelo de Plan Estratégico de los Sistemas para la Gestión y Organización a través de una Plataforma Informática.* Alicante: Editorial Ciencias.

Fonseca Luna, O. (2011). *Sistema de Control Interno para Organizaciones.* Lima: Editorial IICO.

Garrison, D., Anderson,, T., & Archer, W. (2000). *Critical Thinking and Computer Conferencing: A Model and Tool to Assess Cognitive Presence*. Recuperado el enero de 2017, de http://www.atl.ualberta.ca/cmc/CogPresPaper_June30_.pdf

Godoy Ruíz , S. E. (2014). Implementación del Modelo de Itil V3 para la Unidad de Soporte Tecnológico de la Universidad de San Buenaventura, Bogotá. *Trabajo de grado para optar al título profesional de ingeniera de sistemas. [En línea]. Disponible desde: http://biblioteca.usbbog.edu.co:8080/Biblioteca/BDigital/80464.pdf*. Bogotá: Universidad De San Buenaventura .

Gutiérrez , J. (2017). *Guía de implementación de gestión de servicio de TI usando ITIL en las MIPYME.* Bogotá: Escuela colombiana de ingeniría Julio Garavito.

Hernandez. (2017). *Auditoria Informática: Un Enfoque Metodológico y Practico.* México: Editorial Continental.

(2017). Auditoria en informatica : Un enfoque metodológico y práctico. En E. Hernández, *Auditoria en informatica : Un enfoque metodológico y práctico* (pág. p. 315). Mexico: Editorial Continental.

Herrera, M. (24 de abril de 2014). *Una breve mirada a la e p s en ecuador cooperativas de ahorro y crédito cifras y datos.* Recuperado el 15 de marzo de 2019, de https://mpht.wordpress.com/2018/04/24/una-breve-mirada-a-la-e-p-s-en-ecuador-cooperativas-de-ahorro-y-credito-cifras-y-datos/

Hunnebeck, L. (2011). *ITIL Service Design 2011 Edition, the StationerOffice* (2a ed. ed.). Londrés.

ICONTEC. (12 de julio de 2006). *Norma Técnica Colombiana NTC-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).* Recuperado el 15 de marzo de 2019, de http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Illescas, Y. (2013). *En Tungurahua hay Cooperativas de Ahorro como piedras en el río.* Quito.

International Organization for Standardization. (2012). *Business continuity management systems.* Estados Unidos: ISO.

ISACA . (2012). *COBIT 5. A Business Framework for The Governance and Management of Enterprise IT.* ISACA Knowledge Center.

IT GOVERNANCE INSTITUTE. (2008). *ISACA*. Recuperado el 11 de 2018, de Alineando Cobit 4.1, ITIL V3 e ISO/IEC 27002 en Beneficio del Negocio: https://m.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

La Junta de Política y Regulación Monetaria Financiera. (13 de 02 de 2015). *Junta de Regulacion Monetaria Financiera*. Recuperado el 01 de 01 de 2019, de Resolución No. 038-2015-F el 13 de febrero de 2015: http://www.seps.gob.ec/documents/20181/25522/resolucion208-2016f.pdf/790f876f-cae6-405e-90f6-60aa3f175f26

Machado, C., & Torres, P. (2016). Proceso de gestión de problemas para las aplicaciones Core del Banco Falabella a través de la metodología ITIL. *Tesis de especialización*. Bogotá, Colombia: Universidad Católica.

Mera Gómez, A. (2015). Control interno crediticio y su impacto en los resultados financieros del Banco Nacional de Fomento Sucursal Ambato durante el segundo semestre del año 2010. *Tesis inédita*. Ambato: Universidad Técnica de Ambato.

Mohamed, J. (2013). *The drivers of ITIL adoption in uniten, ieee, selangor.* malaysia.

Morán Abad, L., & Pérez Sánchez, l. (2016). *ISO/IEC 20000. Guía completa de aplicación para la gestión de los servicios de tecnologías de la información.* Asociación Española de Normalización y Certificación).

Muñoz Razo, C. (2014). *Auditoría de Sistemas Computacionales.* México: Editorial Pearson.

Ochoa, U., & Alberto, R. (2013)). Diseño e implementación de los procesos de, cumplimiento de solicitudes y gestión de incidentes basados en ITIL versión 3 en la empresa SINERGYTEAM. *Doctoral dissertation*. qUITO: espe.

OGC. (2011). *ITIL , Mejora Continua del Servicio. En ITIL , Mejora Continua del Servicio.* Londres: Editorial TSO.

OGC. (2011). *ITIL Service Operation. En OGC, ITIL Service Operation.* Londres: TSO.

Pérez Villamizar, M. Á. (2018). Aplicación de la metodología ITIL para impulsar la gestión de TI en empresas del Norte de Santander (Colombia): revisión del estado del arte. *Revista Espacios. [En línea]. Recuperado desde: https://www.revistaespacios.com/a18v*

39n09/a18v39n09p17.pdf, Vol. 39(Nº 09), p. 17 .

Piattini velthuis, M. (2014). *Auditoria de tecnologías y sistemas de información.* Navarro: Editorial ALFAOMEGA RA-MA.

Pinilla Forero, J. (2016). *Auditoria Informática: Un Enfoque Operacional.* Colombia: Ecoe Ediciones.

Quintero, L. (2015). Modelo basado en ITIL para la Gestión de los Servicios de TI en la Cooperativa de Caficultores de Manizales. *Tesis de maestría*. Colombia: Universidad Autónoma de Manizales.

SAAC. (2018). *Ecuador: Las cooperativas de ahorro y crédito son las que colocan más recursos.* Quito: El telegrafo.

SEPS. (2019). *Nueva Segmentación Sector Financiero Popular y Solidario*. Obtenido de Seper Intedencia de Economia Popular y Solidaria: http://www.seps.gob.ec/noticia?nueva-segmentacion-sector-financiero-popular-y-solidario

SEPS. (31 de 01 de 2019). *PRODUCTOS ESTADISTICOS*. Recuperado el 15 de 02 de 2019, de BOLETINES FINANCIEROS MENSUALES: http://www.seps.gob.ec/estadistica?boletines-financieros-mensuales

SEPS. (31 de enero de 2019). *SEPS*. Recuperado el 15 de 12 de 2019, de Superintedencia de Economía Popular y Solidaria: https://www.seps.gob.ec/documents/20181/25522/SEPS%20IGT%20IR%20IGJ%202018%200279.pdf/40639c6b-f0d7-4c3c-825e-c4f666e55ccf

Seyal, A. H., Sheung, H., & sharul, T. (2016). A preliminary Evaluation of ICT Centers Performance Using COBIT Framework: Evidence from Institutions of Higher Learning in Brunei Darussalam. En *Computational Intelligence in Information Systems* (págs. 235-243). Springer.

Solares Soto , P., Baca Urbina, G., & Acosta Gonzaga, E. (2014). *Administración Informática I: Análisis y Evaluación de Tecnologías de Información.* México: Editorial Patria.

Superintendencia de Bancos y Seguros. (20 de octubre de 2005). “Normas generales para la aplicación de la ley general de instituciones del sistema financiero”. *resolución No JB-2005-834*. QUito.

Superintendencia de Economía Popular y Solidaria (SEPS). (2018). *Una mirada al desarrollo de la econonomía popular y solidaria.* Boletín - SEPS.

Tirado, M. (2014). Las políticas de crédito y cobranzas y su incidencia en la liquidez de la Fábrica de calzado FADICALZA. *Trabajo de graduación previo a la obtención del título de economista*. Ambato: Universidad Técnica De Ambato.

Zea, M., & Beatriz, D. (2015). *Mejoramiento de la Gestión de Cambios de los Sistemas Informáticos en el Ministerio de Finanzas del Ecuador Aplicando el Proceso de Gestión de Cambios de Itil.* Bogotá.

ANEXO

Anexo 1. Listado de cooperativas de ahorro y crédito del segmento 1

ENTIDAD	DÓLARES	%
Juventud Ecuatoriana Progresista Ltda	1,943,030,999	19.88%
Jardín Azuayo Ltda	864,032,859	8.84%
Policía Nacional Ltda	769,070,206	7.87%
Cooprogreso Ltda	511,376,013	5.23%
29 De Octubre Ltda	499,042,719	5.11%
Oscus Ltda	379,555,546	3.88%
San Francisco Ltda	334,664,380	3.42%
Alianza Del Valle Ltda	316,906,446	3.24%
De La Pequeña Empresa De Cotopaxi Ltda	305,573,748	3.13%
Riobamba Ltda	304,394,877	3.11%
Vicentina Manuel Esteban Godoy Ortega Ltda	287,808,722	2.94%
Andalucia Ltda	255,322,792	2.61%
De La Pequeña Empresa Biblian Ltda	231,084,759	2.36%
Mushuc Runa Ltda	228,044,375	2.33%
Caja Central Financoop	206,189,375	2.11%
Tulcan Ltda	201,235,203	2.06%
El Sagrario Ltda	187,088,896	1.91%
Atuntaqui Ltda	186,764,560	1.91%
23 De Julio Ltda	184,129,016	1.88%
Pablo Muñoz Vega Ltda	178,900,642	1.83%
De Los Servidores Públicos Del Ministerio De Educacion Y Cultura	153,333,773	1.57%
San Jose Ltda	152,279,229	1.56%
Cámara De Comercio De Ambato Ltda	149,627,842	1.53%
Fernando Daquilema	145,388,755	1.49%
De La Pequeña Empresa De Pastaza Ltda	138,719,013	1.42%
Chibuleo Ltda	137,526,246	1.41%
Pilahuin Tio Ltda	131,556,980	1.35%
Santa Rosa Ltda	121,971,042	1.25%
Ambato Ltda	114,812,068	1.17%
15 De Abril Ltda	83,281,940	0.85%
Construcción Comercio Y Producción Ltda	71,831,135	0.73%
Total General	**9,774,544,154**	**100.00%**

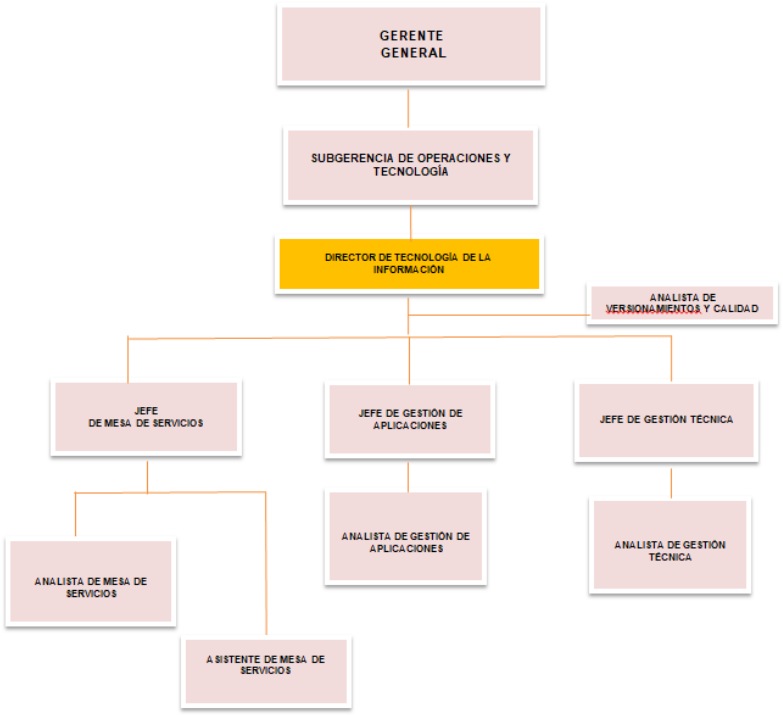
Fuente: (SEPS, 2019)

Anexo 2. Diagnóstico inicial de las COACs de estudio

COOPERATIVAS / INFORMACIÓN	CONVENIO DE CONFIDENCIALIDAD	MISIÓN	VISIÓN	VALORES	ORGANIGRAMA INSTITUCIONAL	PLAN ESTRATÉGICO
MD	X	X	X	X	X	X
GR	X	X	X	X	X	X

Elaboración propia

Anexo 3. Orgánico de la COAC GR



Anexo 4. Orgánico de la COAC MD

Anexo 5. Análisis de los Orgánicos de las COACs

COOPERATIVAS / ORGÁNICOS DE TI	Gerencia	Subgerencia	Dirección	Áreas adicionales	Analistas	Asistentes	TOTAL
GR	1	1	1	3	3	1	10
MD	0	1	1	0	1	1	4

Elaboración propia

Anexo 6. Análisis del Plan estratégico de las COACs

COOPERATIVAS / PLAN ESTRATÉGICO	Objetivos	Análisis de riesgos gestión	FODA	Programas	Indicadores	Responsables	Presupuesto	POA	TOTAL
GR	X	X	X	X	X	X		X	88%
MD	X		X	X			X	X	63%

Elaboración propia

Anexo 7. Análisis del manual de políticas de las COACs

COOPERATIVAS / MANUAL DE POLÍTICAS DE TI	Políticas tecnológicas	Infraestructura de Hardware	Indraestructura de Software	Seguridad	Custodia de equipos	Robo o pérdida	Modificación e instalación de software	Plan de contingencia	Administración de cambios	Políticas de información	Presupuesto	Proveedores	Incidentes	TOTAL
GR	X	X	X	X	X	X	X	X	X	X				77%
MD	X		X	X			X		X	X	X	X	X	69%

Elaboración propia

Anexo 8. Marco referencial COBIT 5 – ITIL V3 – ISO 27002

		ITIL V3 /Procesos / Áreas																											
		Estrategia de Servicio (ES)				Diseño de Servicio (DS)										Transición de Servicio (TS)						Operación de Servicio (OS)					Mejora continua de Servicios (MCS)		
COBIT - Dominios / procesos		Generación de la estrat	Gestión Financiera TI	Gestión de Demanda	Gestión de portafolio de	Gestión de servicios nue	Gestón de catálogo de s	Gestión de niveles de se	Gestión de capacidad	Gestión e disponibilidad	Gestión de continuidad	Gestión de seguridad TI	Gestión de Proveedores	Gestión de Riesgo	Gestión de Arquitectura	Gestión de soporte y tra	Gestión de cambios	Gestión de configuració	Gestión de entregas y w	Gestión de validación	Gestión de conocimient	Gestión de eventos	Gestión de incidencias	Gestión de peticiones	Getsión de problemas	Gestión de acceso	Proceso de mejora en 7	Informes de servicio	Medición de servicio
Evaluar, Orientar y Supervisar (EDM)	Asegurar el establecimiento y mantenimiento del marco de gobierno																												
	Asegurar la entrega de beneficios																												
	Asegurar la optimización de riesgo											X		X															
	Aegurar la optimización de los recursos												X																
	Asegurar la transparencia hacia las partes																												
Objetivos		Directrices de la Dirección en seguridad de la información				Requisitos de negocio para el control de	Gestión de acceso de usuario.	Control de acceso a sistemas y				Seguridad en los procesos de desarrollo y soporte		Areas Seguras	Seguridad de los Equipos	Responsabilidad sobre los Activos	Clasificacion de la Informacion	Manejo de los soportes de almacenamiento	Protección contra código malicioso			Gestión de la seguridad en las redes.	Intercambio de información con partes externas.		Protección contra código malicioso	Copias de seguridad			
ISO 27002 /Dominios		Políticas de Seguridad				Control de Acceso						Adquisición, desarrollo y mantenimiento de los sistemas de información		Seguridad física y ambiental		Gestión de activos						Seguridad en las Telecomunicaciones			Seguridad Operativa				

		ITIL V3 /Procesos / Áreas																											
COBIT – Dominios *I* procesos		Estrategia de Servicio (ES)				Diseño de Servicio (DS)									Transición de Servicio (TS)						Operación de Servicio (OS)					Mejora continua de Servicios		
		Generación de la estrat	Gestión Financiera TI	Gestión de Demanda	Gestión de portafolio	Gestión de servicios a	Gestión de catálogo de	Gestión de niveles de :	Gestión de capacidad	Gestión e disponibilid	Gestión de continuidad	Gestión de seguridad	Gestión de Proveedore	Gestión de Riesgo	Gestión de Arquitectu	Gestión de soporte y l	Gestión de cambios	Gestión de configurac	Gestión de entregas y	Gestión de validación	Gestión de conocimie	Gestión de eventos	Gestión de incidencias	Gestión de peticiones	Getsión de problemas	Gestión de acceso	Proceso de mejora en	Informes de servicio	Medición de servicio
Alinear, Planear y Organizar (APO)	Gestionar el Marco de Gestión de TI	X									X																		
	Gestionar la Estrategia	X																											
	Gestionar la Arquitectura Empresarial														X														
	Gestionar la Innovación						X																						
	Gestionar el Portafolio				X																								
	Gestionar el Presupuesto y los Costes		X																										
	Gestionar los Recursos Humanos																												
	Gestionar las relaciones																												
	Gestionar los acuerdos de						X	X																					
	Gestionar los Proveedores												X																
	Gestionar la Calidad																										X		
	Gestionar el Riesgo													X															
	Gestionar la Seguridad											X																	
Objetivos		Directrices de la Dirección en seguridad de la información				Requisitos de negocio para el	Gestión de acceso de usuario.	Control de acceso a sistemas y				Seguridad en los procesos de desarrollo y soporte		Areas Seguras	Seguridad de los Equipos	Responsabilidad sobre los Activos	Clasificacion de la Informacion	Manejo de los soportes de almacenamiento	Protección contra código malicioso			Gestión de la seguridad en las redes.	Intercambio de información con partes externas.		Protección contra código malicioso	Copias de seguridad			
ISO 27002 /Dominios		Políticas de Seguridad				Control de Acceso						Adquisición, desarrollo y mantenimiento de los sistemas de		Seguridad física y ambiental		Gestión de activos						Seguridad en las Telecomunicaciones			Seguridad Operativa				

		ITIL V3 /Procesos / Áreas																											
COBIT – Dominios *I* procesos		Estrategia de Servicio (ES)				Diseño de Servicio (DS)									Transición de Servicio (TS)						Operación de Servicio (OS)					Mejora continua de Servicios		
		Generación de la estrat	Gestión Financiera TI	Gestión de Demanda	Gestión de portafolio	Gestión de servicios a	Gestión de catálogo d	Gestión de niveles de	Gestión de capacidad	Gestión e disponibilid	Gestión de continuidad	Gestión de seguridad	Gestión de Proveedore	Gestión de Riesgo	Gestión de Arquitectu	Gestión de soporte y	Gestión de cambios	Gestión de configuraci	Gestión de entregas y	Gestión de validación	Gestión de conocimien	Gestión de eventos	Gestión de incidencias	Gestión de peticiones	Gestión de problemas	Gestión de acceso	Proceso de mejora en	Informes de servicio	Medición de servicio
Construir, Adquirir e Implementar (BAI)	Gestión de Programas y Proyectos						X																						
	Gestionar la Definición de Requisitos																												
	Gestionar la Identificación y Construcción de Soluciones														X				X										
	Gestionar la Disponibilidad y la Capacidad								X	X	X							X	X				X						
	Gestionar la Facilitación del Cambio																												
	Gestionar los Cambios																X												
	Gestionar la Aceptación del Cambio y la Transición																X			X									
	Gestionar el Conocimiento																				X								
	Gestionar los																	X	X										
	Gestionar la Configuración																	X											
Objetivos		Directrices de la Dirección en seguridad de la información				Requisitos de negocio para el	Gestión de acceso de usuario.	Control de acceso a sistemas y				Seguridad en los procesos de desarrollo y soporte			Áreas Seguras	Seguridad de los Equipos	Responsabilidad sobre los Activos	Clasificacion de la Informacion	Manejo de los soportes de almacenamiento	Protección contra código malicioso			Gestión de la seguridad en las redes.	Intercambio de información con partes externas.		Protección contra código malicioso	Copias de seguridad			
ISO 27002 /Dominios		Políticas de Seguridad				Control de Acceso						Adquisición, desarrollo y mantenimiento de los sistemas de			Seguridad física y ambiental		Gestión de activos					Seguridad en las Telecomunicaciones			Seguridad Operativa				

		ITIL V3 /Procesos / Áreas																										
COBIT – Dominios / procesos		Estrategia de Servicio (ES)				Diseño de Servicio (DS)										Transición de Servicio (TS)						Operación de Servicio (OS)					Mejora continua de Servicios		
		Generación de la estra	Gestión Financiera TI	Gestión de Demanda	Gestión de portafolio	Gestión de servicios n	Gestión de catálogo d	Gestión de niveles de :	Gestión de capacidad	Gestión e disponibilid	Gestión de continuidad	Gestión de seguridad	Gestión de Proveedore	Gestión de Riesgo	Gestión de Arquitectur	Gestión de soporte y	Gestión de cambios	Gestión de configuraci	Gestión de entregas y	Gestión de validación	Gestión de conocimien	Gestión de eventos	Gestión de incidencias	Gestión de peticiones	Getsión de problemas	Gestión de acceso	Proceso de mejora en	Informes de servicio	Medición de servicio
Entregar, Dar Servicio y Soporte (DSS)	Gestionar Operaciones																					X						
	Gestionar Peticiones e Incidentes de																						X					
	Gestionar Problemas																								X			
	Gestionar la Continuidad										X																	
	Gestionar Servicios de Seguridad											X																
	Gestionar Controles de Proceso de Negocio															X												
Supervisar, Evaluar y Valorar (MEA)	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad																											X
	Supervisar, Evaluar y Valorar el Sistema de Control Interno																										X	
	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos																										X	
Objetivos		Directrices de la Dirección en seguridad de la información				Requisitos de negocio para el	Gestión de acceso de usuario.	Control de acceso a sistemas y				Seguridad en los procesos de desarrollo y soporte		Areas Seguras	Seguridad de los Equipos	Responsabilidad sobre los Activos	Clasificacion de la Informacion	Manejo de los soportes de almacenamiento	Protección contra código malicioso			Gestión de la seguridad en las redes.	Intercambio de información con partes externas.		Protección contra código malicioso	Copias de seguridad			
ISO 27002 /Dominios		Políticas de Seguridad				Control de Acceso						Adquisición , desarrollo y mantenimiento de los sistemas de		Seguridad física y ambiental		Gestión de activos						Seguridad en las Telecomunicaciones			Seguridad Operativa				

Anexo 9. Preguntas según proceso y dominio de TI

EVALUACIÓN			
DOMINIO	COD	PROCESO	ITEM
Evaluar, Orientar y Supervisar (EDM)	EDM1	ORGANIGRAMA DE DECISIÓN	Definido de manera precisa un organigrama donde se establezca quienes son los responsables de tomar las decisiones relacionadas con la planificación, implantación y explotación de TI
	EDM2	DEFINICIÓN DE FUNCIONES	Definido de manera precisa las funciones que deben realizar cada uno de los directivos y técnicos responsables de la planificación, implantación y explotación de TI
	EDM3	DEFINICIÓN DE PROCESOS DE GESTION	Si se tienen definidos los procesos de gestión de las TI
	EDM4	POLÍTICAS DE SEGURIDAD	Definidas conjunto de políticas para la seguridad de la información acorde a las necesidades de la COAC
	EDM5		Revisión periódica de las políticas para la seguridad de la información para su retroalimentación permanente
PROMEDIO POR DOMINIO EDM			

EVALUACIÓN			
DOMINIO	**COD**	**PROCESO**	**ITEM**
Alinear, Planear y Organizar (APO)	APO 1	GESTIÓN DE OPERACIONES	Control de acceso a sistemas y aplicaciones
	APO2	DEFINICIÓN DE PRESTACION DE SERVICIOS	Si se tienen definidos los niveles de prestación de servicios TI
	APO 3	APOYO A LA GESTIÓN ADMINISTRATIVA	Satisfación de los usuarios con la dotación de infraestructuras y servicios TIC de apoyo a los procesos administrativos.
	APO 4	PROCEDIMIENTOS DE ADQUISICIÓN	Si se tienen definidos procedimientos para la adquisición de aplicaciones e infraestructuras.
	APO 5	GESTIÓN FINANCIERA	Dentro de la Prestación de Servicios tiene definida la gestión financiera de manera que conoce el coste de los servicios TI y le sirve de base para deciciones de gestión y análisis de inversiones relativas a TI
	APO 6	GESTIÓN DE RIESGOS	Si se dispone de una metodología y se gestionan los riesgos: plan de contingencias, seguridad, etc.
	APO 7		Protección contra el código malicioso y descargable
	APO 8		Realiza copias de seguridad permanentes que garanticen la fiabilidad de la información
PROMEDIO POR DOMINIO APO			

EVALUACIÓN			
DOMINIO	**COD**	**PROCESO**	**ITEM**
Construir, Adquirir e Implementar (BAI)	BAI1	GESTTIÓN DE OPERACIONES	Control de acceso a las redes y servicios asociados.
	BAI2	GESTIÓN DE LA CAPACIDAD	La Prestación de Servicios tiene asegurada la capacidad de las infraestructuras TI y están alineadas con las necesidades de las COAC
	BAI3	GESTIÓN DE DISPONIBILIDAD	LIa Prestación de Servicios gestiona la disponibilidad de manera que se optimiza la infraestructura y la organización TI para llevar a cabo una prestación de servicios con niveles de disponibilidad sostenible
	BAI4	GESTIÓN DE CAMBIOS	Realiza gestión de cambios garantizando que se usan métodos y procedimientos estandarizados en el manejo eficiente de todos los cambios, para minimizar su posible impacto adverso sobre la calidad del servicio.
	BAI5		Existe una política establecida para la revisión posterior a la implementación de cambios
	BAI6		Esta disponible a este nivel la documentación para establecer el impacto y recursos del Cambio
	BAI7	GESTIÓN DE CONFIGURACIÓN	Realiza gestión de la configuración proporcionando un modelo lógico de la infraestructura TI por medio de la identificación, control, mantenimiento y verificación de las versiones de todos los elementos
	BAI8	PROCEDIMIENTOS DE MANTENIMIENTO	Si se tienen definidos procedimientos para el mantenimiento de aplicaciones e infraestructuras.
	BAI9	GESTIÓN DE VERSIONES	Realiza gestión de versiones disponiendo de una visión integral de las actualizaciones sobre los servicios TI y asegurando que todos los aspectos de una versión, tanto técnicos como no técnicos
	BAI10	DESARROLLO DE SOFTWARE	Si se dispone de una metodología para el desarrollo de software propio.
	BAI11		Registros de administración, operación y fallos
	BAI12		Responsabilidad sobre los Activos
PROMEDIO POR DOMINIO BAI			

EVALUACIÓN			
DOMINIO	**COD**	**PROCESO**	**ITEM**
Entregar, Dar Servicio y Soporte (DSS)	DSS1	GESTIÓN DE NIVELES DE SERVICIO	Gestión de la vulnerabilidad técnica
	DSS2		Tiene definido los niveles de prestación de servicio para mantener y mejorar gradualmente la calidad de los servicios TI
	DSS3	GESTIÓN DE LA CONTINUIDAD	La Prestación de Servicios tiene definida la continuidad de los servicios TI
	DSS4		Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información
	DSS5	GESTIÓN DE PROBLEMAS	Realiza gestión de problemas minimizando el impacto sobre la organización de los errores en las infraestructuras TI y preveniendo de forma proactiva la recurrencia de incidencias relacionadas con dichos errores.
	DSS6	GESTIÓN DE INCIDENCIAS	Realiza gestión de incidencias consiguiendo restaurar la operación normal del servicio lo más rapidamente posible, con el menor impacto para el negocio y el usuario y al menor coste efectivo.
	DSS7		Prevención del uso indebido de los recursos de tratamiento de la información
			Los registros de cambios son analizados para identificar problemas
	DSS8		Satisfación de los usuarios con el nivel de servicio proporcionado en la gestión de incidencias TI
	DSS9	GESTIÓN DE LA SEGURIDAD	Si además de los mínimos legales establecidos, se dispone de una gestión integral de la seguridad.
	DSS10		Gestión de la vulnerabilidad técnica
PROMEDIO POR DOMINIO DSS			

EVALUACIÓN			
DOMINIO	**COD**	**PROCESO**	**ITEM**
Supervisar, Evaluar y Valorar (MEA)	**MEA1**	**GESTIÓN DE LA CALIDAD**	Tienen definidas acciones relacionadas con la gestión de la calidad de los servicios TI: autoevaluación, certificaciones y auditorias.
	MEA2		Supervisión del uso del sistema
	MEA3		Protección de la información de los registros
PROMEDIO POR DOMINIO DSS			

Anexo 10. Modelo de Evaluación de Gestión de Riesgo según COBIT5 – ITILV3 – ISO 27002

MODELO DE EVALUACIÓN DE GESTIÓN DE RIESGO

Herramienta de Evaluación y Diagnóstico bajo COBIT - ITIL - ISO 27002

NOMBRE DE LA COAC:	COOPERATIVA DE AHORRO Y CRÉDITO 29 DE OCTUBRE

EVALUACIÓN				CUMPLIMIENTO (%)						INDICADORES		
DOMINIO	COD	PROCESO	ITEM	GERENTE	CARGO 2	CARGO 3	CARGO 4	CARGO 5	PROMEDIO DE CUMPLIMIENTO	ITEM INDICADOR	VALOR	CÁLCULO INDICADOR
Evaluar, Orientar y Supervisar (EDM)	EDM1	ORGANIGRAMA DE DECISIÓN	Definido de manera precisa un organigrama donde se establezca quienes son los responsables de tomar las decisiones relacionadas con la planificación, implantación y explotación de TI	20	25	36	45	25	30.2	N° de personas en áreas de TI que producen beneficio directo a la COAC	5	56%
	EDM2	DEFINICIÓN DE FUNCIONES	Definido de manera precisa las funciones que deben realizar cada uno de los directivos y técnicos responsables de la planificación, implantación y explotación de TI	35	68	14	12	63	38.4			
	EDM3	DEFINICIÓN DE PROCESOS DE GESTION	Si se tienen definidos los procesos de gestión de las TI	65	78	45	45	87	64.0	N° Total de personas que laboran en el área de TI	9	
	EDM4	POLÍTICAS DE SEGURIDAD	Definidas conjunto de políticas para la seguridad de la información acorde a las necesidades de la COAC	85	95	78	78	98	86.8			
	EDM5		Revisión periódica de las políticas para la seguridad de la información para su retroalimentación permanente	95	100	12	74	45	65.2			
PROMEDIO POR DOMINIO EDM				60.0	73.2	37.0	50.8	63.6	56.9			56%

EVALUACIÓN				CUMPLIMIENTO (%)						INDICADORES		
DOMINIO	COD	PROCESO	ITEM	GERENTE	CARGO 2	CARGO 3	CARGO 4	CARGO 5	PROMEDIO DE CUMPLIMIENTO	ITEM INDICADOR	VALOR	CÁLCULO INDICADOR
Alinear, Planear y Organizar (APO)	APO 1	GESTIÓN DE OPERACIONES	Control de acceso a sistemas y aplicaciones	25	47				36.0	N° de soluciones tecnológicas que no estan alineadas cn la estrategia de la COAC	35	45%
	APO2	DEFINICIÓN DE PRESTACION DE SERVICIOS	Si se tienen definidos los niveles de prestación de servicios TI	63	87				75.0			
	APO 3	APOYO A LA GESTIÓN ADMINISTRATIVA	Satisfación de los usuarios con la dotación de infraestructuras y servicios TIC de apoyo a los procesos administrativos.	14	45				29.5			
	APO 4	PROCEDIMIENTOS DE ADQUISICIÓN	Si se tienen definidos procedimientos para la adquisición de aplicaciones e infraestructuras.	87	96				91.5			
	APO 5	GESTIÓN FINANCIERA	Dentro de la Prestación de Servicios tiene definida la gestión financiera de manera que conoce el coste de los servicios TI y le sirve de base para deciciones de gestión y análisis de inversiones relativas a TI	95	32				63.5	Cantidad de requerimientos tecnológicos requeridos para la estrategia de la COAC	78	
	APO 6	GESTIÓN DE RIESGOS	Si se dispone de una metodología y se gestionan los riesgos: plan de contingencias, seguridad, etc.	48	14				31.0			
	APO 7		Protección contra el código malicioso y descargable	52	58				55.0			
	APO 8		Realiza copias de seguridad permanentes que garanticen la fiabilidad de la información	78	25				51.5			
PROMEDIO POR DOMINIO APO				57.8	50.5	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!	54.1			45%

EVALUACIÓN				CUMPLIMIENTO (%)						INDICADORES		
DOMINIO	COD	PROCESO	ITEM	GERENTE	CARGO 2	CARGO 3	CARGO 4	CARGO 5	PROMEDIO DE CUMPLIMIENTO	ITEM INDICADOR	VALOR	CÁLCULO INDICADOR
Construir, Adquirir e Implementar (BAI)	BAI1	GESTTIÓN DE OPERACIONES	Control de acceso a las redes y servicios asociados.	35					35.0	Total de cambios, instalaciones, configuraciones realizados (mensual)	5	100%
	BAI2	GESTIÓN DE LA CAPACIDAD	La Prestación de Servicios tiene asegurada la capacidad de las infraestructuras TI y están alineadas con las necesidades de las COAC	64					64.0			
	BAI3	GESTIÓN DE DISPONIBILIDAD	Lla Prestación de Servicios gestiona la disponibilidad de manera que se optimiza la infraestructura y la organización TI para llevar a cabo una prestación de servicios con niveles de disponibilidad sostenible	87					87.0			
	BAI4	GESTIÓN DE CAMBIOS	Realiza gestión de cambios garantizando que se usan métodos y procedimientos estandarizados en el manejo eficiente de todos los cambios, para minimizar su posible impacto adverso sobre la calidad del servicio.	95					95.0	N° de cambios, instalaciones, configuraciones fallidas (mensual)	5	
	BAI5		Existe una política establecida para la revisión posterior a la implementación de cambios	100					100.0			
	BAI6		Esta disponible a este nivel la documentación para establecer el impacto y recursos del Cambio	78					78.0			
	BAI7	GESTIÓN DE CONFIGURACIÓN	Realiza gestión de la configuración proporcionando un modelo lógico de la infraestructura TI por medio de la identificación, control, mantenimiento y verificación de las versiones de todos los elementos	42					42.0			
	BAI8	PROCEDIMIENTOS DE MANTENIMIENTO	Si se tienen definidos procedimientos para el mantenimiento de aplicaciones e infraestructuras.	35					35.0	N° de equipos que han recibido mantenimiento (anual)	5	5%
	BAI9	GESTIÓN DE VERSIONES	Realiza gestión de versiones disponiendo de una visión integral de las actualizaciones sobre los servicios TI y asegurando que todos los aspectos de una versión, tanto técnicos como no técnicos	20					20.0	Total de equipos (anual)	110	
	BAI10	DESARROLLO DE SOFTWARE	Si se dispone de una metodología para el desarrollo de software propio.	14					14.0	N° de software realizados por el equipo de TI (anual)	6	
	BAI11		Registros de administración, operación y fallos	85					85.0			
	BAI12		Responsabilidad sobre los Activos	96					96.0			
PROMEDIO POR DOMINIO BAI				62.6	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!	62.6			52%

EVALUACIÓN				CUMPLIMIENTO (%)						INDICADORES		
DOMINIO	COD	PROCESO	ITEM	GERENTE	CARGO 2	CARGO 3	CARGO 4	CARGO 5	PROMEDIO DE CUMPLIMIENTO	ITEM INDICADOR	VALOR	CÁLCULO INDICADOR
Entregar, Dar Servicio y Soporte (DSS)	DSS1	GESTIÓN DE NIVELES DE SERVICIO	Gestión de la vulnerabilidad técnica	36	25				30.5	Cantidad de incidencias RESUELTAS de sistemas caídos por capacidad o desempeño de procesamiento insuficiente (mensual)	2	67%
	DSS2		Tiene definido los niveles de prestación de servicio para mantener y mejorar gradualmente la calidad de los servicios TI	87	36				61.5			
	DSS3	GESTIÓN DE LA CONTINUIDAD	La Prestación de Servicios tiene definida la continuidad de los servicios TI	48	58				53.0			
	DSS4		Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	95	69				82.0	TOTAL de incidencias DENUNCIADAS de sistemas caídos por capacidad o desempeño de procesamiento insuficiente (mensual)	3	
	DSS5	GESTIÓN DE PROBLEMAS	Realiza gestión de problemas minimizando el impacto sobre la organización de los errores en las infraestructuras TI y preveniendo de forma proactiva la recurrencia de incidencias relacionadas con dichos errores.	85	78				81.5			
	DSS6	GESTIÓN DE INCIDENCIAS	Realiza gestión de incidencias consiguiendo restaurar la operación normal del servicio lo más rapidamente posible, con el menor impacto para el negocio y el usuario y al menor coste efectivo.	78	45				61.5			
	DSS7		Prevención del uso indebido de los recursos de tratamiento de la información	41	12				26.5			
			Los registros de cambios son analizados para identificar problemas	14	85				49.5			
	DSS8		Satisfación de los usuarios con el nivel de servicio proporcionado en la gestión de incidencias TI	25	96				60.5			
	DSS9	GESTIÓN DE LA SEGURIDAD	Si además de los mínimos legales establecidos, se dispone de una gestión integral de la seguridad.	23	52				37.5	N°. De vulnerabilidades reportadas		
	DSS10		Gestión de la vulnerabilidad técnica	65	53				59.0	N°. De vulnerabilidades cubiertas		
PROMEDIO POR DOMINIO DSS				54.3	55.4	¡DIV/0!	¡DIV/0!	¡DIV/0!	54.8			67%

EVALUACIÓN				CUMPLIMIENTO (%)						INDICADORES		
DOMINIO	COD	PROCESO	ITEM	GERENTE	CARGO 2	CARGO 3	CARGO 4	CARGO 5	PROMEDIO DE CUMPLIMIENTO	ITEM INDICADOR	VALOR	CÁLCULO INDICADOR
Supervisar, Evaluar y Valorar (MEA)	MEA1	GESTIÓN DE LA CALIDAD	Tienen definidas acciones relacionadas con la gestión de la calidad de los servicios TI: autoevaluación, certificaciones y auditorías.	25					25.0	N°. De auditorías realizadas en el año	1	100%
	MEA2		Supervisión del uso del sistema	98					98.0	N° de sistemnas auditados	15	43%
	MEA3		Protección de la información de los registros	78					78.0	Total de sistemas existentes en la COAC	35	
PROMEDIO POR DOMINIO DSS				67.0	¡DIV/0!	¡DIV/0!	¡DIV/0!	¡DIV/0!	67.0			71%

Elaboración propia