ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRIA EN EVALUACION Y AUDITORIA EN SISTEMAS TECNOLOGICOS

IV PROMOCION

TESIS DE GRADO DE MAESTRIA EN EVALUACION Y AUDITORIA EN SISTEMAS TECNOLOGICOS

TEMA: "DESARROLLO DE UN MODELO DE MADUREZ TECNOLÓGICO PARA CATEGORIZAR A LAS INSTITUCIONES FINANCIERAS, DE LOS SEGMENTOS 3 Y 4 DE LA SUPERINTENDENCIA ECONOMÍA POPULAR Y SOLIDARIA ("SEPS")".

AUTORES: BAYAS, MÓNICA ISABEL
LOZADA, WILLIAM GIOVANNY

DIRECTOR: ING. TRUJILLO, NIKOLAY MBA.

SANGOLQUÍ, MAYO 2014.

CERTIFICADO

Certifico que el presente trabajo fue realizado en su totalidad por los Señores Ingenieros MONICA ISABEL BAYAS CONDO y WILLIAM GIOVANNY LOZADA SANCHEZ, como requerimiento parcial a la obtención del Título de MAGISTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS.

Sangolquí, 22 de mayo de 2014.

Ing. Moisés Nikolay Trujillo Avilés, MBA
DIRECTOR DEL PROYECTO

DECLARACION DE RESPONSABILIDAD

Nosotros, MONICA ISABEL BAYAS CONDO y WILLIAM GIOVANNY LOZADA SANCHEZ, declaramos bajo juramento que el presente proyecto de grado denominado, "DESARROLLO DE UN MODELO DE MADUREZ TECNOLÓGICO PARA CATEGORIZAR A LAS INSTITUCIONES FINANCIERAS, DE LOS SEGMENTOS 3 Y 4 DE LA SUPERINTENDENCIA ECONOMÍA POPULAR Y SOLIDARIA ("SEPS")", es de nuestra autoría; y no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento, respetando derechos intelectuales de terceros, cuyas fuentes se incorporan en la bibliografía.

Sangolquí, 22 de mayo de 2014.

Ing. Mónica Isabel Bayas Condo CC. 1803235157	Ing. William Giovanny Lozada Sánchez CC. 1803437969

AUTORIZACIÓN

Nosotros, Mónica Isabel Bayas Condo y William Giovanny Lozada Sánchez, Autorizamos a la UNIVERSIDAD DE LAS FUERZAS ARMADAS -ESPE, la publicación en la biblioteca virtual de la institución, de la tesis de grado titulada: "Desarrollo de un modelo de madurez tecnológico para categorizar a las Instituciones Financieras, de los segmentos 3 y 4 de la Superintendencia Economía Popular y Solidaria ("SEPS")", cuyo contenido, idea y criterios son de nuestra responsabilidad y autoría.

Sangolquí, 22 de Mayo de 2014.

Ing. Mónica Isabel Bayas Condo CC. 1803235157	Ing. William Giovanny Lozada Sánchez CC. 1803437969

AGRADECIMIENTO

Nuestro principal agradecimiento a Dios, por permitirnos día a día luchar por los sueños, brindándonos la fortaleza, la paciencia y la tenacidad para enfrentar cada uno de los obstáculos y hoy lograr una meta más en nuestras vidas.

A la UNIVERSIDAD DE LAS FUERZAS ARMADAS –ESPE, por abrirnos las puertas para afianzar nuestra formación y crecimiento tanto personal como profesional.

De la misma manera un agradecimiento especial al Ing. Nikolay Trujillo, MBA director de nuestro trabajo, por su aporte invaluable.

DEDICATORIA

.

A nuestros padres y hermanos quienes con su amor, apoyo y comprensión incondicional estuvieron siempre a lo largo de este caminar; a ellos que siempre tuvieron una palabra de aliento en los momentos difíciles y que han sido fortaleza de nuestras vidas, de la misma manera a cada una de las personas que nos han apoyado en el desarrollo de nuestra vida profesional.

Mónica y William

INDICE GENERAL

INDICE DE CUADROS

INDICE DE GRAFICOS

RESUMEN

El presente trabajo permitió desarrollar un Modelo para determinar el nivel de madurez de las instituciones financieras, a través de la evaluación de la capacidad de los procesos de TI, brindando a la Superintendencia de Economía Popular y Solidaria una herramienta a través de la cual se puede obtener una visión global de la situación real dentro de las organizaciones bajo su supervisión y control, para en un futuro generar acciones que permitan el fortalecimiento tanto de sus procesos de revisión como ente de control al igual que la gestión dentro de las organizaciones supervisadas. En el desarrollo del modelo se identificaron los procesos de tecnología con mayor grado de importancia, y a partir de ellos se elaboró la metodología para el diagnóstico y evaluación de capacidad. El modelo fue sometido a evaluación a través de la ejecución de una prueba piloto en una institución financiera perteneciente al segmento 3, obteniendo oportunidades de mejora para la organización así como también para el modelo, con los resultados alcanzados se generaron recomendaciones para fortalecer la gestión de los procesos de tecnología, y de la misma manera fue posible determinar el nivel de madurez en el que se encuentra la organización.

Palabras Clave: Modelo de madurez, capacidad, COBIT, procesos, evaluación.

ABSTRACT

This work allowed us to develop a model to determine the level of maturity of financial institutions, through capacity assessment of IT processes, providing to the Superintendency of Popular and Solidarity Economy a tool through which it can obtain an overview of the actual situation within organizations under its supervision and control, for in a future generate actions that allow the strengthening so much of its processes of review as entity of control, as the management inside the supervised organizations. In the model development process technology with greater importance were identified, and from them the methodology for the diagnosis and evaluation of capacity was developed. The model was subjected to evaluation through the implementation of a pilot project in one belonging to segment 3 financial institution, obtaining improvement opportunities for the organization as well as for the model with the results obtained recommendations were generated to strengthen the management of technology processes, and in the same way it was possible to determine the level of maturity in which the organization is located..

Keywords: Maturity Model, capability, COBIT, processes, evaluation.

CAPITULO I

1.1 Introducción

La información y la tecnología que la soporta, representan los activos más valiosos en las empresas hoy en día, aunque la principal problemática es el comprender la importancia de esta sinergia.

La SEPS como parte de sus competencias y entendiendo la importancia de las tecnologías de la información ("TI") dentro de las organizaciones, pone a disposición normativa que aporte al logro de objetivos y la continuidad del negocio, donde se exhorta al cumplimiento de los principios de integridad, confidencialidad y disponibilidad, en los procesos de captura, procesamiento, almacenamiento y transmisión de la información, de una manera oportuna, ágil y confiable.

Con base a la afirmación realizada la presente tiene como objetivo desarrollar de un modelo que permita, tanto a la SEPS como a las organizaciones supervisadas, conocer su realidad actual a través de una evaluación de la capacidad de los procesos de tecnología.

Para la determinación del modelo de madurez se desarrollará un método de evaluación basado en la calificación de la capacidad de los procesos para que una organización pueda identificarse con una escala de niveles de 0 a 5.

Las escalas definidas para el Modelo de Madurez ayudarán a determinar deficiencias en la administración de TI y a fijarse objetivos que permitan una adecuada gestión en las organizaciones aplicando las referencias provistas por las mejores prácticas y la normativa legal.

1.2 Justificación e Importancia

El desarrollo de un modelo de madurez brindará a la SEPS, una herramienta de evaluación alineada a la realidad de las organizaciones controladas, y su aplicación busca la detección de las deficiencias en la administración de TI, el grado de aplicación de acuerdo a las directrices brindadas y en el seguimiento de objetivos.

Como parte de las entidades controladas el aplicar la evaluación a través del modelo de madurez les permitirá conocer el nivel de madurez en el que se encuentran, brindándoles con esto oportunidades de mejora tanto a nivel de procesos de tecnología como procesos de negocio.

De la misma manera, la aplicación del modelo propuesto dentro de las entidades entregará a la SEPS, resultados que pueden convertirse en una oportunidad de mejora a través de la revisión y generación de normativa legal y controles de supervisión focalizados directamente los puntos con mayor deficiencia.

1.2.1 Estado del arte a nivel mundial y local

De acuerdo al punto de vista que quiera aplicarse para conocer el nivel en el que se encuentra una organización, se han ido abriendo paso distintas metodologías y modelos aplicables, de esta manera se puede mencionar los siguientes modelos de madurez: *Process and Enterprise Maturity Model* (PEMM™) de Michael Hammer (Saffirio, 2008), *Sofware Engineering Institute* denominado *Capability Maturity Model* (Saffirio, 2008), *Capability Maturity Model* de COBIT 4.1 de ISACA, y con un enfoque de evaluación de capacidad de procesos el *Process Assessment*

Model(PAM) presente en la versión COBIT 5, que le permitirán a la organización ir creciendo de manera estructurada, planeada y balanceada.

1.3 Planteamiento del problema

La Superintendencia de Economía Popular y Solidaria tiene entre sus competencias la supervisión y control de las entidades que conforman el Sector Financiero Popular y Solidario, y parte de estas competencias consiste en velar por la estabilidad, solidez y correcto funcionamiento de estas entidades a través de la evaluación periódica.

Al momento no existe un modelo de madurez que permita categorizar e identificar a las entidades de acuerdo a la capacidad y fortaleza de su ambiente tecnológico, por lo tanto no se pueden tomar acciones y controles en función de casos o sectores que requieran atención proactiva sino solamente hasta después de la realización de un examen integral.

Las tecnologías de la información forman parte del riesgo operativo de una organización perteneciente al Sector Financiero Popular y Solidario, y entendiéndose como riesgo la probabilidad de que ocurra un evento que afecte de manera negativa o positiva al normal funcionamiento de esta, aparece sin lugar a dudas la oportunidad de desarrollar un modelo de madurez.

1.4 Formulación del problema a resolver

- **Problema General**
  - ¿Cómo se podría categorizar a una organización en función de la capacidad de sus procesos tecnológico?
- **Problemas Específicos**
  - ¿Cuáles son los procesos tecnológicos de mayor relevancia e impacto en las entidades del sector Financiero Popular y Solidario?
  - ¿A qué procesos de tecnología en las organizaciones se valorará su grado de madurez?
  - ¿Cómo se plantea realizar la valoración de los procesos de tecnología de las organizaciones?
  - ¿Cuál es el fin de valorar los procesos tecnológicos en las instituciones bajo la supervisión y control de la SEPS?

1.5 Objetivo General

Desarrollar un modelo de madurez tecnológico para categorizar a las Instituciones Financieras, de los segmentos 3 y 4 bajo la supervisión de la Superintendencia Economía Popular y Solidaria (“SEPS”) para identificar oportunidades de mejora tanto en normativa legal como en los procesos de supervisión y control.

1.6 Objetivos Específicos

- Determinar los procesos tecnológicos con mayor relevancia e impacto en las organizaciones del sector Financiero Popular y Solidario.

- Definir aquellos procesos con mayor influencia en las organizaciones supervisadas a los cuales se determinará su grado de madurez.

- Integrar varios marcos de referencia que sirvan de base para el desarrollo de un Modelo de Madurez Tecnológico para evaluar la madurez de los procesos de tecnología alineados a los propósitos de supervisión y control de la SEPS.

- Categorizar y agrupar a las organizaciones, según el nivel o grado de madurez de los procesos tecnológicos con el fin de identificar oportunidades de mejora tanto en normativa legal como en los procesos de supervisión y control.

CAPITULO II

2.1 Marco teórico.

2.1.1 Estado del arte

Los modelos de Madurez a nivel mundial, se han ido adaptando conforme la necesidad de las organizaciones llegando incluso a combinaciones que dan origen a nuevos modelos de madurez como el que proponen Villegas (Villegas, Viloria, & Blanco) donde se hace un enfoque hacia la Seguridad de la Información caracterizando principalmente al contexto de las Organizaciones Inteligentes, este modelo trae consigo sus propios niveles de valoración adaptados al ámbito en el que se realiza el estudio.

Dentro del Centro Interamericano de Administraciones Tributarias, se propone también el desarrollo de un Modelo de Madurez de los Procesos de TI, principalmente para conocer la capacidad técnica de sus asociados, inspirados en el marco de referencia COBIT, y el modelo de madurez de CMMI.

Pero no únicamente los modelos de madurez han evolucionado hacia el área tecnológica sino que ha tocado ámbitos como el Riesgo Empresarial, al cual también Machado y Ramírez (Machado & Ramirez, 2012) le plantearon el desarrollo de un modelo de madurez de capacidad de la gestión de riesgos, tomando como marco de referencia COSO ERM, donde su objetivo primordial es mejorar la gestión en las organizaciones pero punto primordial a través del manejo del riesgo.

Del lado de la educación también se ha planteado el desarrollo de modelos de madurez de los procesos apoyados en las Tecnologías de la Información Rivera y

Álvarez (Rivera G. & Alvarez G, 2012), proponen realizar la evaluación del grado de madurez a través de tres dimensiones (procesos, servicios y soporte TI) que evaluadas en conjunto (Procesos Vs Servicios y Procesos Vs servicios Vs Soporte TI) permitiendo conocer el estado actual de dichas instituciones en cuanto al nivel de calidad y eficiencia de sus procesos esenciales, A nivel nacional se ha identificado trabajos que hacen referencia también a los modelos de madurez dentro de la educación, pero esta vez enfocándose en la enseñanza virtual (Cano, et al., 2012), donde se toma como punto de análisis varios modelos existentes que cubren el E-learning, destacando los aportes que más impacto podrían tener en un planteamiento de un modelo especifico que responda a la enseñanza virtual actual.

2.1.2 Marco teórico

2.1.2.1 Superintendencia de Economía Popular y Solidaria (SEPS).

La nueva Constitución del Ecuador aprobada en Montecristi en el año 2008, definió cambios sustanciales para el tratamiento de la economía del país, introduciendo un nuevo concepto de Economía Popular y Solidaria.

La Economía Popular y Solidaria involucra directamente al Sistema Financiero, y está regulada a través de la Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario (LOEPS) y su Reglamento (SEPS, 2011).

Dicha ley consta de dos pilares fundamentales:

1. Nuevo modelo institucional del sector: dividiendo en dos segmentos la economía: el sector real compuesto por los sectores comunitarios, asociativos, cooperativos (excepto de ahorro y crédito) y las unidades económicas populares (UEP).

2. El sector financiero popular y solidario (SFPS), integrado por cooperativas de ahorro y crédito (COAC), entidades asociativas o solidarias, cajas y bancos comunales, y cajas de ahorro.

La Superintendencia de Economía Popular y Solidaria es una entidad técnica de supervisión y control de las organizaciones de la economía popular y solidaria, que busca el desarrollo, estabilidad, solidez y correcto funcionamiento del sector económico popular y solidario.

2.1.2.1.1 Segmentación de las organizaciones.

La Ley Orgánica de la Economía Popular y Solidaria del Sector Financiero Popular y Solidario, en sus artículos 101 y 145 párrafo segundo (SEPS, 2011), establece que las Cooperativas de Ahorro y Crédito deben ser ubicadas en segmentos, con el fin de generar políticas y regulaciones dependiendo de sus características particulares, entre las que se mencionan: participación en el sector, volumen de operaciones que desarrollen, número de socios, número y ubicación geográfica de oficinas operativas a nivel local cantonal, provincial, regional o nacional; monto de activos; patrimonios; productos y servicios financieros.

Según la resolución No. JR-STE-2012003 emitida por la Junta de Regulación del Sector Financiero Popular y Solidario (Junta de Regulacion del SFPS, 2012), se establece la ubicación de las cooperativas de ahorro y crédito en los segmentos: uno, dos, tres, según las características definidas en la Tabla 1, tomado en cuenta el siguiente orden de prioridad: los activos, número de cantones en los que opera y número de socios, de la siguiente manera:

Segmento	Activos (USD)	Cantones	Socios
Segmento 1	0 - 250.000,00	1	más de 700
Segmento 1	0 - 1'100.000,00	1	hasta 700
Segmento 2	250.000,01 - 1'100.000,00	1	más de 700
Segmento 2	0 - 1'100.000,00	2 o más	Sin importar el número de socios
Segmento 2	1'100.000,01 - 9'600.000,00	Sin importar el número de cantones en que opera	hasta 7.100
Segmento 3	1'100.000,01 o mas	Sin importar el número de cantones en que opera	más de 7.100
Segmento 3	9'600.000,01 o más	Sin importar el número de cantones en que opera	Hasta 7.100

Figura 1: Parámetros de Segmentación de la SEPS **(RSFPS, 2012)**

El segmento cuatro lo componen las COACs, que se hallaban bajo el control de la Superintendencia de Bancos y Seguros “SBS”.

2.1.2.1.2 Sector Financiero Popular y Solidario

El sector financiero popular y solidario está compuesto por cooperativas de ahorro y crédito, entidades asociativas o solidarias, cajas y bancos comunales, cajas de ahorro. Se establece que las iniciativas de servicios del sector financiero popular y solidario y de las micro, pequeñas y medianas unidades productivas, recibirán un tratamiento diferenciado y preferencial del Estado, en la medida en que impulsen el desarrollo de la economía popular y solidaria. (Ediciones Legales Informacion Adicional).

2.1.2.2 Riesgo Operativo.

El riesgo operativo en una organización se entenderá como la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en

los procesos, personas, tecnología de información y por eventos externos. (Superintendencia de Bancos y Seguros).

2.1.2.2.1 Factores del Riesgo Operativo:

Con el propósito de minimizar la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, se deben tener en cuenta varios aspectos, según manifiesta la normativa legal emitida por la Superintendencia de Bancos y Seguros, para la gestión del riesgo operativo en el componente de Tecnologías de Información (Superintendencia de Bancos y Seguros),

A través del análisis de la normativa legal, se han identificado los factores y procesos de tecnología que forman parte de la gestión del riesgo operativo, los cuales se detallan a continuación:

- **Factor:** Garantizar la administración en la tecnología de información, debe soportar adecuadamente los requerimientos de operación actuales y futuros de la Entidad.

Proceso TI	Descripción
Compromiso del Directorio y la alta Gerencia.	Apoyo y compromiso del Directorio y de la alta Gerencia.
Plan funcional de tecnología.	El plan debe estar alineado con el plan estratégico institucional y el plan operativo, con el fin de asegurar el encaminamiento de la Entidad.

Tecnología de Información.	Registrar el volumen y monitoreo de transacciones, sin dejar de lado el crecimiento de la Entidad.
Administrador de cambios	Debe existir una persona responsable de los cambios realizados, para controlar y asegurar la correcta ejecución de la aplicación.
Políticas, procesos y procedimientos de tecnología de información	Manual de Políticas, procesos y procedimientos de tecnología de información, alineado con las actividades y objetivos de la Entidad, a fin de garantizar la ejecución de los criterios internos de eficacia, eficiencia y cumplimiento, debidamente aprobados por el directorio
Difusión de Políticas, procesos y procedimientos de tecnología de información	El personal debe conocer las políticas, procesos y procedimientos de tecnología de información, para asegurar la implementación
Capacitación y entrenamiento técnico	Capacitación y entrenamiento al personal y a los usuarios del área de tecnología.

- **Factor:** Garantizar que las operaciones de tecnología de información, satisfagan los requerimientos de la entidad.

Proceso TI	**Descripción**
Manuales y Reglamento interno	Los manuales y reglamentos debidamente aprobados por la alta gerencia, teniendo en cuenta las responsabilidades y procedimientos

	para el uso de las instalaciones y respuestas a incidentes de la tecnología de información.
Registro e identificación de los activos de tecnología de información.	Clasificación, registro e identificación de los activos, sin dejar de lado el responsable del mismo.

- **Factor:** Garantizar que los recursos y servicios provistos por terceros, se administren con responsabilidad y sean sometidas a un monitoreo de su eficiencia y efectividad.

Proceso TI	Descripción
Propiedad de la información y de las aplicaciones.	Responsabilidades de la empresa proveedora, con el fin de conservar la integridad, disponibilidad y confidencialidad de la información, en caso de que sus aplicaciones sean vulnerables.
Aplicaciones parametrizadas.	Garantizar la transferencia de conocimiento, por medio de documentación técnica detallada, con el fin de reducir la dependencia entre la entidad y la empresa proveedora.

- **Factor:** Garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad, para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas.

Proceso TI	Descripción
Políticas y procedimientos de seguridad de la información	Estableciendo sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas.
Identificación de los requerimientos de seguridad relacionados con la tecnología de información.	Debe contener principalmente: la evaluación de los riesgos que enfrenta la institución; los requisitos legales, normativos, reglamentarios y contractuales; y, el conjunto específico de principios, objetivos y condiciones para el procesamiento de la información que respalda sus operaciones.
Asegurar la integridad, disponibilidad y confidencialidad de la información	Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada.
Seguridades en el acceso a la información	Un sistema de administración que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría; además de los controles necesarios que permitan verificar su cumplimiento en todos los ambientes de procesamiento.
Niveles de autorización de accesos y ejecución de las funciones de	Niveles de autorización de accesos y ejecución de las funciones de

procesamiento de las aplicaciones	procesamiento de las aplicaciones, para garantizar la segregación de funciones y reduzcan el riesgo de error o fraude.
Sistemas de control y autenticación	Controles adecuados para evitar accesos no autorizados, inclusive de terceros; y, ataques externos especialmente a la información crítica y a las instalaciones de procesamiento.
Detectar y evitar la instalación de software	Controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software maliciosos.
Proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos externos	Controles formales para proteger la información y el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores.
Procesamiento de información crítica en áreas protegida	Suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida.
Condiciones físicas y ambientales	Las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la

	infraestructura de tecnología de información.
Sistema de administración de la seguridad de la información.	Plan para evaluar el desempeño del sistema de administración, que permita tomar acciones orientadas a mejorarlo.
Servicios de transferencias y transacciones electrónicas	Las instituciones que ofrezcan los servicios de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad de la información que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro, mediante técnicas de encriptación de información; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría.

- **Factor**: Garantizar la continuidad de las operaciones.

Proceso TI	Descripción
Minimizar riesgos potenciales	Minimizar imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; polvo; interrupciones en el fluido eléctrico, desastres naturales; entre otros.
Políticas y procedimientos de respaldo	La información crítica pueda ser

de información periódicos.	recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado.
Sistemas de comunicación y redundancia	Mantener sistemas que permitan garantizar la continuidad de sus servicios.
Respaldos y procedimientos de restauración en una ubicación remota	Garantizar la disponibilidad ante eventos de desastre en el centro principal de procesamiento, de manera remota.

- **Factor**: Garantizar el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones que satisfagan los objetivos del negocio.

Proceso TI	Descripción
Administración y control de los procesos.	Una metodología que permita controlar el proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados.
Documentación técnica y de usuario.	La documentación debe estar permanentemente actualizada de las aplicaciones de la institución, a fin de preservar los conocimientos y el manejo de las aplicaciones.
Versionamiento de aplicaciones.	Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción.

Calidad de la información.	Controles que aseguren la calidad de la información en la migración, cumpliendo características de integridad, disponibilidad y confidencialidad.

- **Factor: Eventos Externos**

En la administración del riesgo operativo, las instituciones deben considerar la posibilidad de pérdidas derivadas por eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.

2.1.2.3 Marco de Referencia COBIT 5

Evolución.- El proyecto COBIT se emprendió por primera vez en el año 1995, con el fin de crear un mayor producto global que pudiese tener un impacto duradero sobre el campo de visión de los negocios, así como sobre los controles de los sistemas de información implantados. (Ortega de la Torre)

La primera edición fue publicada en 1996, la segunda edición en 1998, la tercera edición en 2000, la edición en línea en 2003, la cuarta edición en 2005, la versión 4.1 en 2007, la versión 5 abril 10/2012.

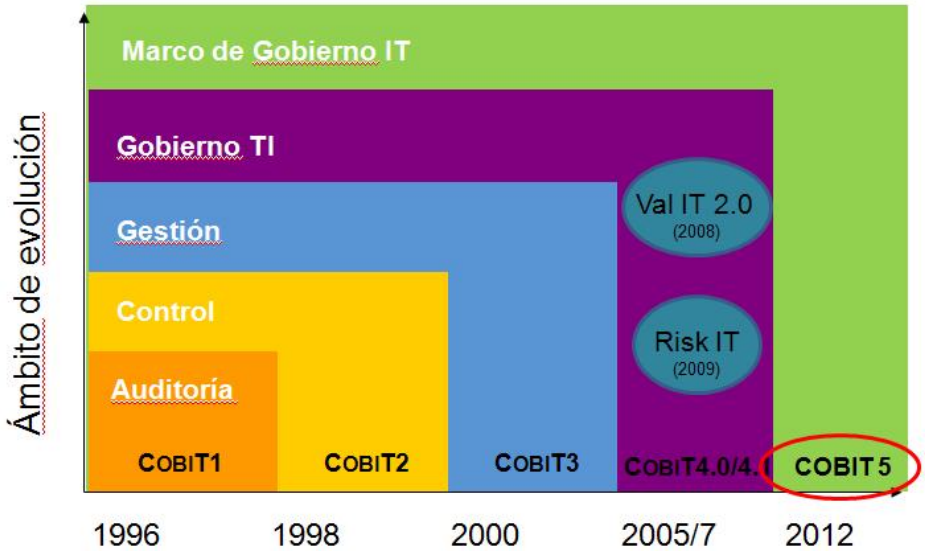


Figura 2: Evolución de COBIT **(Crisoltic, 2012)**

Cobit es uno de los marcos de trabajo más importantes y aceptados a nivel mundial, para la adecuada implementación de Gobierno TI. Además es un conjunto de buenas prácticas que permite el desarrollo de políticas claras en las organizaciones.

2.1.2.3.1 Principios de Cobit:

1. **Satisfacer las necesidades del accionista.-** corresponden a las estrategias accionables de la organización, es decir, traducen las necesidades de las partes interesadas como: la realización de servicios, optimización de riesgos, optimización de recursos, dentro de las metas de organización, luego pasan a metas relacionadas y finalmente en metas habilitadoras.

   Creación de Valor.- mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y la utilización de recursos. (Cedeno, 2012)

2. **Considerar la empresa de punta a punta.-** no solo se toma en cuenta las funciones, sino también la tecnología como un activo, que puede ser manejado por otro activo de la organización.

3. **Aplicar un único modelo de referencia integrado.-** está alineado con otros marcos y normas, que son utilizados en las organizaciones, a fin de integrar el marco de gobierno y administración:

   - Corporativo: COSO, COSO ERM,
   - Relacionado con TI: ITIL, PMBOK, CMMI
   - Seguridad: ISO27001
   - Calidad: ISO 9001.

4. **Posibilitar un enfoque holístico.-** impulsados por las metas en cascada ya sea por factores individuales o colectivos, es decir, se define qué metas organizaciones deben ser relacionadas con los diferentes habilitadores para saber qué se debía lograr.

   Habilitadores de Cobit: (Sperat)

   1. Principios, políticas y modelos de referencia
   2. Procesos
   3. Estructuras organizacionales
   4. Cultura, ética y comportamiento
   5. Información
   6. Servicios, infraestructura y aplicaciones

7. Gente, habilidades y competencias.

Figura 3: Habilitadores de COBIT5 **(Cedeno, 2012)**.

5. **Separar gobierno de la gestión.-** se distingue claramente entre el Gobierno y la Gestión.

- **Gobierno**.- evalúa las necesidades, condiciones y opciones de las partes interesadas para determinar el alcance de las metas corporativas (equilibradas y acordadas), estableciendo la dirección a través de la priorización y la toma de decisiones por medio de la medición del rendimiento y el cumplimiento.

  El gobierno es responsabilidad del consejo de administración bajo la dirección de su presidente.

- **Gestión.-** la gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el gobierno para alcanzar las metas empresariales.

La gestión es responsabilidad de la dirección ejecutiva bajo la dirección del CEO.

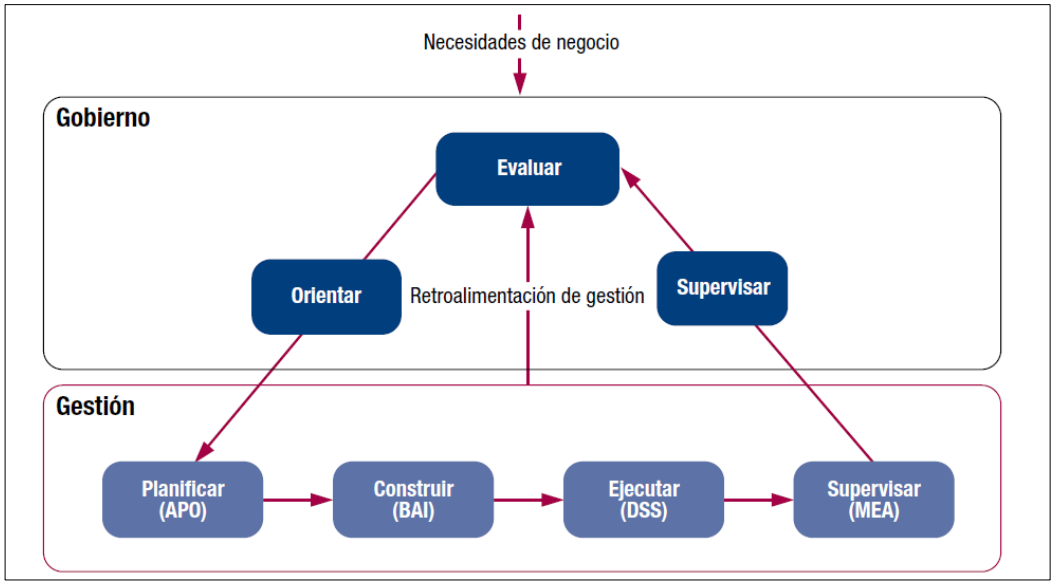


Figura 4: Las Áreas Clave de Gobierno y Gestión de COBIT 5 **(ISACA.ORG)**

2.1.2.3.2 Dominios:

El modelo de referencia COBIT 5 distingue entre el Gobierno y la Gestión, razón por la cual se dividen los dominios según su estructura y los diferentes propósitos:

- **Gobierno.-** está estructurado por un dominio, conteniendo cinco procesos.

- **Evaluación, orientación y supervisión (EDM).-** evaluar las necesidades de las organización, teniendo en cuenta las condiciones y opciones a fin de monitorear el desempeño, cumplimiento y el progreso comparando con la dirección y objetivos.

- 01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.
- 02 Asegurar la entrega de beneficios.
- 03 Asegurar la optimización del riesgo.
- 04 Asegurar la optimización de recursos.
- 05 Asegurar la transparencia hacia las partes interesadas

- **Gestión.-** está estructurado por cuatro dominios, conteniendo varios procesos detallados a continuación:

1. **Alinear, Planificar y Organizar (APO)**.- contiene 13 procesos que comprenden el uso de la información y la tecnología, para lograr los objetivos y las metas de la compañía, tomando en cuenta la forma de la organización y de infraestructura de TI, para lograr resultados óptimos y generar más beneficios con la utilización de las TI.
   - 01 Gestionar el marco de gestión de TI.
   - 02 Gestionar la estrategia.
   - 03 Gestionar la arquitectura empresarial.
   - 04 Gestionar la innovación.
   - 05 Gestionar el portafolio.
   - 06 Gestionar el presupuesto y los costes.
   - 07 Gestionar los recursos humanos.
   - 08 Gestionar las relaciones.
   - 09 Gestionar los acuerdos de servicio.

- 10 Gestionar los proveedores.
- 11 Gestionar la calidad.
- 12 Gestionar el riesgo.
- 13 Gestionar la seguridad.

2. **Construir, Adquirir e Implementar (BAI).-** está estructurado por 10 procesos y buscan la identificación de requerimientos de TI, adquirir tecnología y la implementación de los procesos de negocio actuales de la organización.
   - 01 Gestionar programas y proyectos.
   - 02 Gestionar la definición de requisitos.
   - 03 Gestionar la identificación y construcción de soluciones.
   - 04 Gestionar la disponibilidad y la capacidad.
   - 05 Gestionar la introducción del cambio organizativo.
   - 06 Gestionar los cambios.
   - 07 Gestionar la aceptación del cambio y la transición.
   - 08 Gestionar el conocimiento.
   - 09 Gestionar los activos.
   - 10 Gestionar la configuración.

3. **Entregar, Servicio y Soporte (DSS).-** contiene 6 procesos, los cuales aseguran la continuidad de la operación desde la gestión, atención de incidentes y problemas, mitigando los riesgos y aportando la seguridad para

que las funciones de soporte de TI se realicen regularmente y en forma adecuada.

- 01 Gestionar operaciones.
- 02 Gestionar peticiones e incidentes de servicio.
- 03 Gestionar problemas.
- 04 Gestionar la continuidad.
- 05 Gestionar servicios de seguridad.
- 06 Gestionar controles de procesos de negocio.

4. **Supervisar, Evaluar y Valorar (MEA)**.- contiene 3 procesos, que permiten evaluar los resultados del sistema de TI, verificando el cumplimiento de objetivos para los cuales fue diseñado y el establecimiento de controles para cumplir con los requerimientos regulatorios. Este dominio también abarca la evaluación de la eficiencia del sistema en su capacidad para cumplir con los objetivos del negocio y los procesos de control.
    - 01 Supervisar, evaluar y valorar el rendimiento y la conformidad.
    - 02 Supervisar, evaluar y valorar el sistema de control interno.
    - 03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

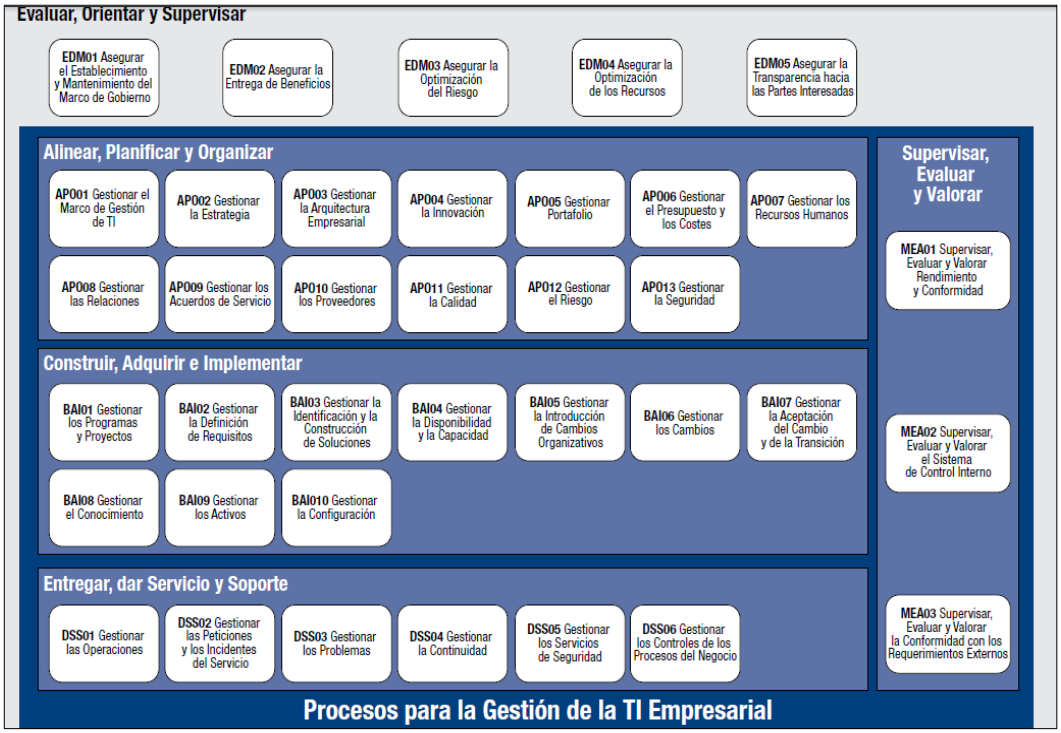


Figura 5: Dominios de Cobit 5 **(ISACA.ORG)**

2.1.2.4 Niveles de Madurez.

El Modelo de Madurez es un conjunto de actividades que permiten obtener un diagnóstico de la situación tecnológica actual y muestra el camino a la mejora de la situación y alcanzar el nivel deseado, conforme la normativa legal a través del mejoramiento continuo de los procesos de la organización.

Existen varios tipos de niveles de madurez, a continuación se detallan los siguientes:

2.1.2.4.1 Modelo de capacidad de los procesos:

Los niveles de capacidad para la evaluación de los procesos, definidos en Cobit 5 son:

0. Proceso incompleto.- el proceso no se ejecuta o no es capaz de lograr su propósito.

1. Proceso alcanzado.- el proceso se lleva a cabo y es capaz de alcanzar sus propósitos.

2. Proceso administrado.- proceso gestionado y establece productos de trabajo que son capaces de mantenerse.

2.1 Administración del desempeño.

2.2 Administración del producto del trabajo.

3. Proceso establecido.- proceso definido basado en un estándar.

3.1 Definición del proceso.

3.2 Desarrollo del proceso.

4. Proceso predecible.- proceso realizado consistentemente en los límites definidos.

4.1 Medición del proceso.

4.2 Control del proceso.

5. Proceso optimizado.- proceso en mejoramiento, a fin de cumplir con los objetivos actuales de la organización y los proyectados.

5.1 Innovación del proceso.

5.2 Optimización del proceso.

A continuación se mostrará un cuadro de comparación entre Cobit 4.1 y Cobit 5, sobre el Modelo de Madurez:

COBIT 4.1	COBIT 5	Contexto
	ISO 15504	
5. Optimizado	5. Optimizado	Empresa / Conocimiento Corporativo
4. Gestionado	4. Predecible	
3. Definido	3. Establecido	
N/A	2. Gestionado	Individual / Conocimiento Individual
N/A	1. Alcanzado	
2. Repetible 1. Ad Hoc 0. No Existente	0. Incompleto	

Figura 6: Comparación entre ambos Modelos de Madurez. **(IT_GRC, Franco)**

2.1.2.5 NORMA ISO 15504.

La Norma ISO/IEC 15504 es una norma internacional, desarrollada por Organización Internacional de Normalización (ISO por sus siglas en ingles *International Organization for Standardization*), en conjunto con la Comisión Electrotécnica Internacional (IEC por sus siglas en ingles *International Electrotechnical Commission***)**, también conocido como *Software Process Improvement Capability Determination* (SPICE) es un modelo para evaluar y mejorar la capacidad y madurez de los procesos, donde la organización obtiene una puntuación a nivel de proceso (Ramirez, 2012).

Características:

- Establece un marco y requisitos para cualquier proceso de evaluación de procesos.
- Proporciona requisitos para los modelos de evaluación de los procesos y modelos de evaluación de organizaciones.
- Proporciona guías para la definición de las competencias de un evaluador de procesos.
- Comprende la evaluación de procesos, mejora de procesos, determinación de capacidad.

Niveles de Capacidad de los Procesos

A continuación en la Figura **7** se muestra un resumen de los Niveles de Capacidad utilizados para la evaluación de los procesos.

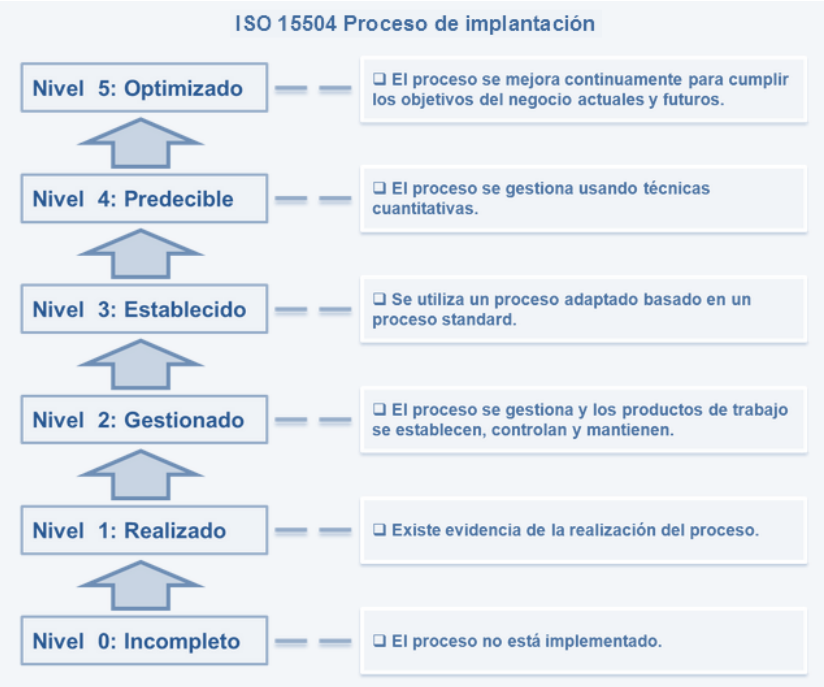


Figura 7: Modelos de Madurez ISO15504 **(INGERTEC)**

2.1.2.6 ISO 27000

La ISO 27000 son una serie estándares que permiten implementar un Sistema de Gestión de Seguridad, que tiene como base la seguridad de la información.

Se persiguen 3 objetivos:

1. Preservar la confidencialidad de los datos de la empresa
2. Conservar la integridad de estos datos
3. Hacer que la información protegida se encuentre disponible

ISO 27001.- es una norma que permite organizar y gestionar la seguridad de la información en la organización, protegiendo información considerada como crítica o relevante. El proceso de seguridad de la información basado en el ciclo de Deming, ciclo de mejora continua o ciclo PDCA (Planear, Hacer, Chequear y Actuar), creando el Sistema de Gestión de la Seguridad de la Información

La norma involucra procesos, gente y tecnología para el análisis y detección de riesgos, permitiendo establecer directrices para eliminarlos o minimizarlos por de las cuatro grandes actividades:

1. Establecer el sistema.
2. Implementar y operar el sistema.
3. Mantener y mejorar el sistema.

4. Monitorear y revisar el sistema.

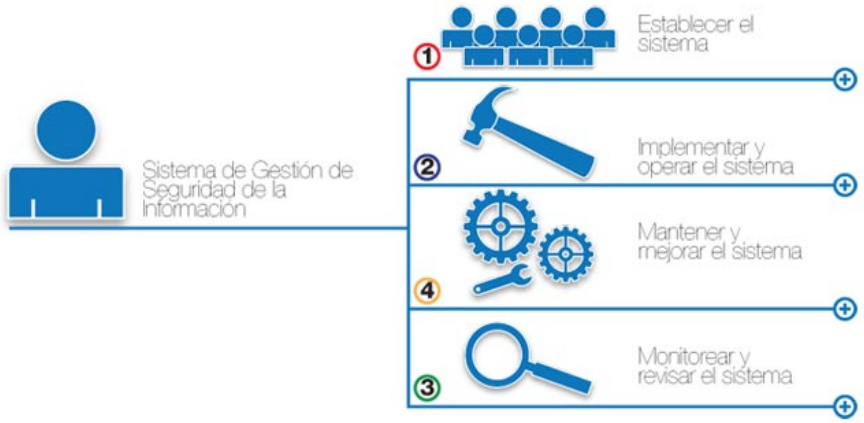


Figura 8: Actividades de la Norma ISO-27001 **(Acevedo Juárez, 2011)**

2.1.2.7 ITIL

Es un conjunto de buenas prácticas desarrollado para apoyar a las organizaciones en el aseguramiento de la calidad y eficiencia en los servicios de TI, sin importar el tipo, dimensión o razón social de la empresa.

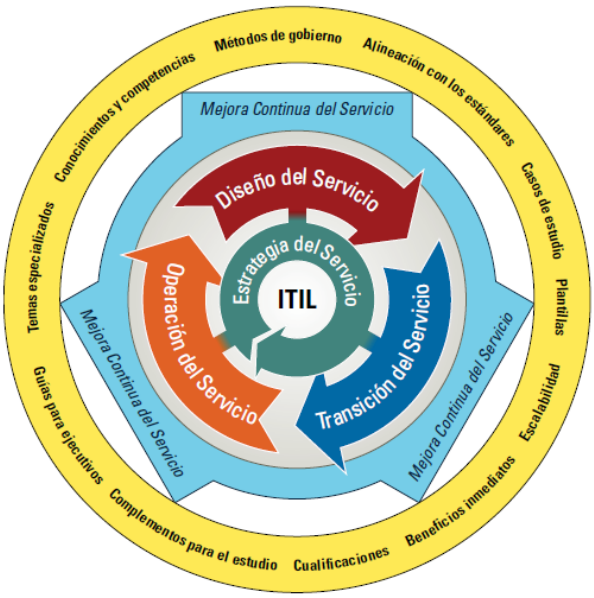


Figura 9: Modelo ITIL V3 **(Taylor & Turbitt)**

Ciclo de vida de los Servicios:

El marco de referencia ITIL, en su versión 3 compuesto por 5 etapas principales, determinadas de la siguiente manera:

- **Estrategia del Servicio.-** trata a la gestión del servicio como una capacidad sino como una gestión de servicio
- **Diseño del Servicio.-**transforma los objetivos estratégicos en portafolios de servicios, ya sea para nuevos o unos ya existentes.
- **Transición del Servicio.-**es el proceso de transición para la implementación de nuevos o existentes servicios.
- **Operación del Servicio.-** cubre las mejores prácticas para la gestión del servicio.
- **Mejora Continua del Servicio**.- permite mejorar los servicios ya existentes en la organización.

Beneficios de ITIL:

- Reducción de gastos.
- Mejoramiento de los servicios TI.
- Mejoramiento en la satisfacción de clientes.
- Normas y orientación.
- Mejora de productividad.

- Mejor utilización de las habilidades y de la experiencia.

- Mejor entrega de los servicios a terceros a través de la especificación de ITIL o ISO 20000 como estándar para la entrega de servicios en los servicios de compras

2.1.3 Marco conceptual

- **COBIT 5** provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. (ISACA.ORG)

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

- **La gestión** planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales. (ISACA.ORG)
- **ISO 27001.-** Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS

7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. (ISO27000)

- **ITIL** es el enfoque más ampliamente aceptado para la gestión de servicios de TI en el mundo. ITIL proporciona un conjunto coherente de las mejores prácticas, procedentes de los sectores público y privado a nivel internacional. (ITIL)

CAPÍTULO III

3.1 Desarrollo del Modelo de Madurez

3.1.1 Definición de los niveles del modelo de madurez.

Los modelos de evaluación son empleados para poder conocer el estado actual de la organización en términos de capacidad de procesos. Además, la identificación de debilidades en los procesos sirve para implementar un proceso de mejora continua (Palomino Vasquez, 2011).

Para la realización de una evaluación de procesos en una empresa es necesario seguir un método de evaluación que produzca resultados cuantitativos que caractericen el rendimiento y la capacidad del proceso (o la madurez de la organización) (Palomino Vasquez, 2011); estos resultados ofrecen información que permite determinar el estado actual de los procesos para encontrar sus fortalezas y debilidades que sirven para definir estrategias para la ejecución de la mejora de procesos.

Para la construcción del presente modelo se ha tomado como fuente primaria la definición de procesos del marco de referencia COBIT 5, junto con uno de sus documentos complementarios Process Assessment Model (PAM), para la evaluación de procesos que a su vez tiene como base la norma ISO/IEC 15504.

También se ha encontrado un gran aporte en el modelo COMPETISOFT (Pino, Serrano, García, Piattini, & Oktaba, 2006), el modelo propuesto por (Pino, Garcia,

Ruiz, & Piattini, 2006), el material preparado por (Garzas, Fernandez, & Piattini, 2009) que también utilizan como base la norma ISO/IEC 15504.

3.1.2 Determinación de los principales procesos de TI.

El papel de la SEPS se enmarca dentro de la supervisión y control, por tal razón se han priorizado los procesos que encajan dentro de este ámbito y sobre los cuales se ejecutará el proceso de evaluación.

Para el presente trabajo se ha construido una matriz de criterios con valores entre 1 a 5, que buscan determinar la importancia de un proceso definido en COBIT 5 para cubrir el objetivo de la SEPS, como se puede visualizar en la tabla 7

Valor	Categoría
1	Sin Importancia
2	Casi sin Importancia
3	Poco Importante
4	Importante
5	Muy importante

Tabla 1: Niveles de Importancia para calificación de procesos.

Únicamente los procesos que se hallen por sobre el valor de 3, serán considerados para evaluación.

3.1.2.1 Dominios y Procesos

DOMINIO	Evaluar, Orientar y Supervisar (EDM)	
Id. Proceso	**Proceso**	**Importancia**
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.	2
EDM02	Asegurar la entrega de beneficios.	2
EDM03	Asegurar la optimización del riesgo.	2
EDM04	Asegurar la optimización de recursos.	2
EDM05	Asegurar la transparencia hacia las partes interesadas.	2

Tabla 2: Evaluación de Procesos Dominio EDM

DOMINIO	Alinear, Planificar y Organizar (APO)	
Id. Proceso	**Proceso**	**Importancia**
APO01	Gestionar el marco de gestión de TI.	4
APO02	Gestionar la estrategia.	3
APO03	Gestionar la arquitectura empresarial.	2
APO04	Gestionar la innovación.	2
APO05	Gestionar el portafolio.	3
APO06	Gestionar el presupuesto y los costes.	2
APO07	Gestionar los recursos humanos.	3
APO08	Gestionar las relaciones.	4
APO09	Gestionar los acuerdos de servicio.	4
APO10	Gestionar los proveedores.	4
APO11	Gestionar la calidad.	2
APO12	Gestionar el riesgo.	4
APO13	Gestionar la seguridad.	5

Tabla 3: Evaluación de Procesos Dominio APO

DOMINIO	Construir, adquirir e implementar (BAI)	
Id. Proceso	**Proceso**	**Importancia**
BAI01	Gestionar programas y proyectos.	2
BAI02	Gestionar la definición de requisitos.	2
BAI03	Gestionar la identificación y construcción de soluciones.	2
BAI04	Gestionar la disponibilidad y la capacidad.	4
BAI05	Gestionar la introducción del cambio organizativo.	2
BAI06	Gestionar los cambios.	4
BAI07	Gestionar la aceptación del cambio y la transición.	4
BAI08	Gestionar el conocimiento.	3
BAI09	Gestionar los activos.	4
BAI10	Gestionar la configuración.	4

Tabla 4: Evaluación de Procesos Dominio BAI

DOMINIO	Entrega, Servicio y Soporte (DSS)	
Id. Proceso	**Proceso**	**Importancia**
DSS01	Gestionar operaciones.	3
DSS02	Gestionar peticiones e incidentes de servicio.	3
DSS03	Gestionar problemas.	4
DSS04	Gestionar la continuidad.	4
DSS05	Gestionar servicios de seguridad.	4
DSS06	Gestionar controles de procesos de negocio.	4

Tabla 5: Evaluación de los Procesos de Dominio DSS

DOMINIO	Supervisar, Evaluar y Valorar (MEA)	
Id. Proceso	**Proceso**	**Importancia**
MEA01	Supervisar, evaluar y valorar el rendimiento y la conformidad.	2
MEA02	Supervisar, evaluar y valorar el sistema de control interno.	4
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos.	2

Tabla 6: Evaluación de los Procesos de Dominio MEA

3.1.2.2 Definición de actividades

A continuación se detallará las actividades que permitirán evaluar el nivel de capacidad de cada uno de los procesos.

3.1.2.2.1 ALINEAR, PLANIFICAR Y ORGANIZAR (APO)

Gestionar el Marco de Gestión de TI
Definir la estructura organizativa. • Verificar que se establezca el alcance, las funciones internas y externas, los roles internos y externos, las capacidades y los derechos incluidas las actividades de TI • Verificar el alineamiento de la organización relativa a TI con los modelos organizativos de arquitectura corporativa (Plan TI). • Verificar que exista un comité estratégico y directivo de TI a fin de revisar, supervisar y realizar seguimiento las inversiones, los niveles de servicio y las mejoras en el servicio.
Establecer roles y responsabilidades. • Verificar que los roles y responsabilidades estén estructurados de

acuerdo a las necesidades y objetivos de organización, a fin de delimitar claramente las responsabilidades y la rendición de cuentas, especialmente para la aprobación y toma de decisiones. • Verificar que se incluya en las descripción de roles y responsabilidades, la adhesión a las políticas y los procedimientos de gestión, al código ético y a las prácticas profesionales. • Verificar que los roles y responsabilidades sean difundidas a todos los empleados de la organización.
Definir la propiedad de la información (datos) y del sistema. • Verificar que existan políticas y directrices para asegurar la adecuada clasificación de la información en la organización. • Verificar que se cree o se mantenga un inventario de la información incluyendo un listado de los propietarios, custodios y clasificaciones. Incluir los sistemas subcontratados y aquellos cuya propiedad debe permanecer dentro de la empresa. • Verificar la implementación de procedimientos para asegurar la integridad y consistencia de la información almacenada en formato electrónico.
Mantener el cumplimiento con las políticas y procedimientos. • Verificar que exista un seguimiento del cumplimiento de las políticas y procedimientos. • Verificar que se analice las tendencias en el funcionamiento y cumplimiento para adoptar las acciones apropiadas.
Gestionar la Estrategia
Evaluar el entorno capacidades y rendimientos actuales. • Verificar el desarrollo un punto de referencia del negocio, entorno de TI, capacidades y servicios actuales respecto al que las necesidades futuras

• Verificar la identificación los actuales y potenciales riesgos y tecnologías en declive. • Verificar la identificación de los problemas, fortalezas, oportunidades y amenazas en el entorno actual, las capacidades y servicios para entender el desempeño actual.
Definir el plan estratégico y la hoja de ruta. • Verificar la identificación y abordaje de los riesgos, costes e implicaciones de los cambios organizativos, evolución tecnológica, requisitos normativos, reingeniería de los procesos de negocio, dotación de personal, oportunidades de internalización y externalización, etc., en el proceso de planificación. • Verificar la hoja de ruta indicando la planificación y las interdependencias de las iniciativas. • Verificar que los objetivos sean representadas por métricas (qué) y objetivos (cuánto) que puedan ser relacionados con los beneficios empresariales. • Verificar la aprobación del plan.
Gestionar el Portafolio
Evaluar y seleccionar los programas a financiar • Verificar las evaluaciones detalladas de los casos del negocio de los programas, evaluando el alineamiento estratégico, beneficios corporativos, riesgo y disponibilidad de recursos. • Verificar el análisis de los programas a ser financiados.
Mantener los portafolios • Verificar la creación y mantenimiento de portafolios de programas de inversiones TI, servicios TI y activos TI, que constituyan la base del presupuesto actual de TI y soporten los planes estratégicos y tácticos de TI.
Gestionar los Recursos Humanos

Mantener la dotación de personal suficiente y adecuada
 	
• Verificar la evaluación de las necesidades de personal :
  o La función de TI cuenta con recursos suficientes para apoyar de manera adecuada y apropiada las metas y objetivos empresariales.
  o La empresa cuenta con recursos suficientes para apoyar de manera adecuada y apropiada los procesos de negocio y los controles e iniciativas TI.
• Verificar que los procesos de contratación y de retención del personal de TI y del negocio estén en línea con las políticas y procedimientos de personal.

Identificar personal clave de TI. • Verificar la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión, el respaldo del personal, el entrenamiento cruzado e iniciativas de rotación de puestos. • Verificar la aprobación de los planes de respaldo del personal.
Gestionar el personal contratado. • Verificar la implementación de políticas y procedimientos que describan cuándo, cómo y qué tipo de trabajo puede ser realizado o incrementado por consultores y/o contratistas, de acuerdo con la política de contratación de TI de la organización y el marco de control de TI. • Verificar los acuerdos formales de los contratistas que están obligados a cumplir con el marco de control de TI de la empresa, tal como políticas de control de seguridad, control de acceso físico y lógico, uso de las instalaciones, requisitos de confidencialidad de la información y los acuerdos de confidencialidad. • Verificar que la definición con el contratista sea clara en sus funciones y responsabilidades como parte de sus contratos, incluidos requisitos explícitos para documentar su trabajo en base a normas y formatos

previamente acordados.
Gestionar las relaciones
Gestionar las relaciones con el negocio. • Verificar la asignación un responsable de cada unidad de negocio. • Verificar que las decisiones claves son acordadas y aprobadas por las partes responsables y relevantes de la organización.
Coordinar y comunicar. • Verificar la coordinación y comunicación de cambios y actividades de transición tales como: proyectos, planes de cambio, planificaciones, políticas de lanzamiento, errores conocidos y concienciación sobre formación. • Verificar a coordinación y comunicación de las actividades operativas, roles y responsabilidades, incluyendo la definición de los tipos de petición, escalado jerárquico, periodos de interrupción significativos (planeados o no) y contenido y frecuencia de los informes del servicio. • Verificar el mantenimiento un plan de comunicación interno a extremo que defina el la relación en la organización.
Gestionar los acuerdos de servicio
Identificar servicios TI. • Verificar la valoración de los servicios TI actuales y los niveles de servicio para identificar falencias existentes en los servicios y los procesos de la organización. • Verificar la que los servicio existentes estén estructurados en nuevos paquetes de servicio, ejecutados, probados y modificados para cumplir con los requisitos de negocio. • Verificar el catálogo de servicios TI regularmente para identificar servicios obsoletos, a fin de acordar la retirada de los mismos y/o proponer cambios.
Catalogar servicios basados en TI.

• Verificar la publicación de los servicios TI, paquetes de servicios y opciones de nivel del servicio activo de la cartera de servicios más relevantes. • Verificar el desarrollo y actualización de los componentes en el portafolio y en los catálogos de servicio.
Definir y preparar acuerdos de servicio. • Verificar los requisitos de los acuerdos de servicios nuevos o modificados desde la gestión de las relaciones con el negocio para asegurar el emparejamiento con los niveles de servicio. Considerar aspectos como tiempos del servicio, disponibilidad, rendimiento, capacidad, seguridad, continuidad, cumplimiento normativo y regulatorio, usabilidad y limitaciones de la demanda. • Verificar los acuerdos operativos internos y acuerdos de servicio con clientes y proveedores.
Supervisar e informar de los niveles de servicio. • Verificar la supervisión y recolección de datos del nivel del servicio. • Verificar que exista informes regulares y formales sobre el rendimiento del acuerdo del servicio, incluyendo desviaciones con respecto a los valores acordados • Verificar los planes de acción y remedio para los incidentes del rendimiento o tendencias negativas del mismo.
Revisar acuerdos de servicio y contratos. • Verificar que existan acuerdos de servicio, bitácoras de cambios en los requisitos, servicios TI, paquetes de servicios u opciones de nivel de servicio.
Gestionar los Proveedores
Identificar y evaluar las relaciones y contratos con proveedores. • Verificar la identificación , registro y categorización de los proveedores y contratos existentes

• Verificar la evaluación del rendimiento de los proveedores, periódicamente.
Gestionar contratos y relaciones con proveedores • Verificar la asignación de propietarios de las relaciones con el proveedor y hacerles responsables de la calidad del servicio proporcionado. • Verificar un proceso de comunicación formal y de revisión, que incluyan las interacciones con el proveedor y la planificación. • Verificar que exista acuerdo, gestión, mantener y renovar los contratos con los proveedores. Asegurando que los contratos estén conformes con las normas corporativas y con los requisitos legales y regulatorios. • Verificar contratos con los proveedores de servicios, para revisar los lugares de trabajo, las prácticas y controles de la dirección o de terceras partes. • Verificar la definición y formalización de los roles y responsabilidades de cada proveedor, cuando varios proveedores se combinan para proporcionar un servicio, considerar asignar un rol de proveedor líder a uno de los proveedores para que asuma la responsabilidad global del contrato.
Gestionar el riesgo en el suministro • Verificar la identificación, supervisión y, cuando sea apropiado, gestionar los riesgos relacionados con la capacidad del proveedor de entregar el servicio de forma eficiente, eficaz, segura, fiable y continua.
Gestionar el Riesgo
Recopilar datos. • Verificar que exista un método para la recolección, clasificación y análisis de datos relacionados con riesgo de TI, dando cabida a múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo. • Verificar el registro de datos sobre los eventos de riesgo que han

causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de TI. • Verificar el registro de eventos de riesgo ocurrido y la forma en la que afecto, la frecuencia del evento y la magnitud de la pérdida. • Verificar la ejecución del análisis periódico de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo y para obtener un entendimiento de los asociados factores de riesgo internos y externos.
Analizar el riesgo. • Verificar la definición de los factores de riesgo y la criticidad en el negocio de los activos. Establecer el alcance del análisis de riesgos después de llevar a cabo un análisis coste-beneficio. • Verificar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual. • Verificar el análisis del coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/ capturar.
Mantener un perfil de riesgo. • Verificar el inventario de procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y externalizados y documentar la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI. • Verificar la capturar de riesgos de TI que se han materializado, para su inclusión en el perfil de riesgo de TI de la organización.
Expresar el riesgo. • Verificar que se informe el análisis de riesgos a todas las partes

afectadas incluyendo probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.
Definir un portafolio de acciones para la gestión de riesgos • Verificar la elaboración un conjunto de propuestas de proyecto diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades estratégicas empresariales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.
Responder al riesgo. • Verificar la categorización de los incidentes y comparar las exposiciones reales con la tolerancia al riesgo. • Verificar que se aplique un plan de respuestas apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.
Gestionar la Seguridad
Establecer y mantener un SGSI. • Verificar la definición de un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología, con un enfoque global de la gestión de la seguridad en la empresa. • Verificar la definición y comunicación de los roles y las responsabilidades de la gestión de la seguridad de la información.
Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. • Verificar que exista un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa.
Supervisar y revisar el SGSI. • Verificar la realización de auditorías internas al SGSI para fortalecer la

seguridad. • Verificar la realización de las revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.

3.1.2.2.2 CONSTRUIR, ADQUIRIR E IMPLEMENTAR (BAI)

Gestionar la disponibilidad y la capacidad.
Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia. • Verificar la creación de una línea de referencia, para la evaluación de disponibilidad, rendimiento y capacidad de servicios y recursos por medio de requisitos del cliente, prioridades de negocio, objetivos de negocio, impacto en el presupuesto, utilización de recursos, capacidades de TI y tendencias de la industria. • Verificar la identificación y seguimiento a los incidentes causados por un rendimiento o una capacidad inadecuados.
Evaluar el impacto en el negocio. • Verificar la identificación de soluciones o servicios que son críticas para los procesos de gestión de la disponibilidad y la capacidad. • Verificar evaluaciones de impacto en el negocio de disponibilidad, rendimiento y capacidad.
Planificar requisitos de servicios nuevos o modificados. • Verificar las implicaciones en la disponibilidad y la capacidad de cambios en las necesidades del negocio y oportunidades de mejora. Utilizando técnicas de modelado para validar los planes de disponibilidad, rendimiento y capacidad. • Verificar la priorización de las necesidades de mejora y crear planes de disponibilidad y capacidad justificables en costes.

Supervisar y revisar la disponibilidad y la capacidad. • Verificar la emisión de la información periódica de los resultados para su revisión por la TI y la gestión del negocio y comunicar a la dirección empresarial. • Verificar la integración de las actividades de supervisión
Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad. • Verificar la identificación de brechas de rendimiento y capacidad sobre la base de la monitorización del rendimiento actual y previsto. • Verificar la integración de las acciones correctivas dentro de los procesos apropiados de planificación y gestión de cambios. • Verificar la definición de un procedimiento para la resolución rápida en emergencias en caso de problemas de capacidad y rendimiento.
Gestionar los cambios.
Evaluar, priorizar y autorizar peticiones de cambio • Verificar la categorización de todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio, recursos necesarios, así como las razones contractuales, legales o de regulación que motivan el cambio. • Verificar la planificación y evaluación de las peticiones de una manera estructurada. • Verificar la aprobación formalmente de los cambios por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser pre-aprobados como cambios estándar. • Verificar la planificación y programar todos los cambios aprobados.
Gestionar cambios de emergencia. • Verificar el procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el

cambio de emergencia. • Verificar que los accesos de emergencia para realizar los cambios están debidamente autorizados y documentados.
Hacer seguimiento e informar de cambios de estado. • Verificar la categorización de las peticiones de cambio en el proceso de seguimiento (ej. rechazados, aprobados pero aún no iniciados, aprobados y en proceso y cerrados). • Verificar la existencia de informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento • Verificar que exista la supervisión de los cambios abiertos para asegurar que los cambios aprobados son cerrados en los plazos previstos, de acuerdo a su prioridad.
Cerrar y documentar los cambios. • Verificar la inclusión de cambios en la documentación (ej. procedimientos de negocio y operativos de TI, documentación de continuidad de negocio y recuperación frente a desastres, información de configuración, documentación de la aplicación, pantallas de ayuda y material de formación). • Verificar la documentación del cambio del sistema antes y después y la documentación de usuario.
Gestionar la Aceptación del Cambio y la Transición
Establecer un plan de implementación. • Verificar el plan de implantación que refleje la estrategia global de implantación, la secuencia de acciones de implantación, recursos necesarios, interdependencias, criterios para la aceptación por parte de la Dirección de la implantación en producción, requisitos para verificar la instalación, estrategia de transición para el soporte en producción, y la actualización de los planes de continuidad de negocio (BCPs). • Verificar que todos los planes de implantación estén aprobados y revisados por la auditoría interna, si es apropiado.

Pasar a producción y gestionar los lanzamientos. • Verificar la existencia de componentes de la solución donde los usuarios son notificados y que la distribución se realiza únicamente a los destinatarios correctamente identificados y autorizados. Incluir procedimientos de marcha atrás en el proceso de lanzamiento para posibilitar la revisión de la distribución de cambios, en caso de error o mal funcionamiento.
• **Gestionar el Conocimiento**
Cultivar y facilitar una cultura de intercambio de conocimientos. • Verificar la existencia de una herramienta que permita almacenar el conocimiento y los elementos que den soporte a la compartición y transferencia de conocimientos.
• Utilizar y compartir el conocimiento. • Verificar la transferencia del conocimiento a los usuarios de conocimientos basándose en un análisis de necesidades, técnicas de aprendizaje efectivas y herramientas de acceso.
Gestionar los Activos
Identificar y registrar los activos actuales. • Verificar la identificación de todos los activos en propiedad en un registro que indique el estado actual. Mantener su alineación con los procesos de gestión de cambios y de la configuración, el sistema de gestión de la configuración y los registros contables financieros. • Verificar la conciliación de todos los activos en propiedad mediante la realización periódica de controles de inventario físicos y lógicos,

Gestionar Activos Críticos. • Verificar la existencia de una categorización de los activos críticos. • Verificar un plan de mantenimiento preventivo para todo el hardware, considerando un análisis coste-beneficio, recomendaciones del proveedor, el riesgo de interrupción del servicio, personal cualificado y otros factores relevantes.
Administrar Licencias. • Verificar un registro de todas las licencias de software adquiridas y sus acuerdos de licencia asociados. • Verificar que el número de copias de software instalado con el número de licencias en propiedad.
Gestionar la configuración
Mantener y controlar los elementos de configuración • Verificar la creación, revisión y formalización de los acuerdos sobre los cambios en las líneas de referencia de configuración cuando sea necesario.

3.1.2.2.3 ENTREGA, SERVICIO Y SOPORTE(DSS)

Gestionar Operaciones
Ejecutar procedimientos operativos • Verificar el desarrollo y mantenimiento de procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados. • Verificar que se cumpla con los estándares de seguridad aplicables para la recepción, procesamiento, almacenamiento y salida de datos de forma tal que se satisfagan los objetivos empresariales, la política de seguridad de la empresa y los requerimientos regulatorios.

• Verificar que se programe, realice y se registre las copias de respaldo de acuerdo con las políticas y procedimientos establecidos.
Gestionar servicios externalizados de TI • Verificar la integración de procesos críticos de la gestión interna de TI, con los proveedores de servicios externalizados cubriendo, por ejemplo, la planificación de la capacidad y el rendimiento, la gestión del cambio, la gestión de la configuración, la gestión de peticiones de servicio y de incidentes, la gestión de problemas, la gestión de la seguridad, la continuidad del negocio y la monitorización y notificación del desempeño de los procesos.
Supervisar la infraestructura de TI • Verificar la identificación y mantenimiento del listado de activos de la infraestructura que necesiten ser monitorizados • Verificar se establezca un procedimientos para supervisar los registros de eventos y llevar a cabo revisiones periódicas. • Verificar el registro oportuno de incidente cuando la monitorización identifica desviaciones de los umbrales definidos.
Gestionar el entorno • Verificar la identificación de los posibles desastres naturales y desastres causados por el ser humano que puedan ocurrir en el área donde se encuentran las instalaciones de TI. • Verificar la implementación de políticas de equipamiento de TI, incluyendo el equipamiento móvil y el ubicado fuera de las instalaciones, áreas sensibles y que se prohíba el almacenamiento de material de oficina y otros suministros que puedan representar un riesgo de incendio en los centros de procesamiento de datos. • Verificar la existencia y mantenimiento periódico de los dispositivos que detectan proactivamente las amenazas del entorno (p. ej. fuego, agua, humo, humedad). • Verificar que exista mantenimiento en todo momento a los sitios de TI y

las salas de servidores limpias y en una condición segura (es decir, sin desorden, sin papel ni cajas de cartón, sin papeleras llenas, sin productos químicos o materiales inflamables).
Gestionar las instalaciones • Verificar que las instalaciones cumplan con regulaciones, directrices y especificaciones de seguridad en el trabajo. • Verificar que exista un plan de estructura de cableado y el *patching* físico (datos y telefonía) están estructurados y organizados. • Verificar el plan de alteraciones físicas a los sitios o localizaciones de TI para reevaluar el riesgo del entorno (p.ej. daño por fuego o agua). Informar los resultados de este análisis a los niveles directivos de continuidad de negocio y de gestión de edificios.
Gestionar peticiones e incidentes de servicios
Definir esquemas de clasificación de incidentes y peticiones de servicio. • Verificar la definición de esquemas y modelos de clasificación de incidentes y peticiones de servicio. • Verificar la definición de reglas para escalado de incidentes.
Registrar, clasificar y priorizar peticiones e incidentes. • Verificar el registro de los incidentes y peticiones de servicio. • Revisar la priorización de peticiones de servicio e incidentes según la definición de impacto en el negocio y la urgencia.
Resolver y recuperase de incidentes. • Verificar el registro de soluciones temporales para resolver los incidentes, si han sido usadas. • Verificar la documentación de la resolución del incidente y evaluar si puede usarse como una fuente de conocimiento en el futuro.
Gestionar problemas.
Resolver y cerrar problemas.

• Verificar el cierre de los registros de problemas, después de la confirmación de la eliminación satisfactoria del error conocido, • Verificar la obtención de informes periódicos de gestión de cambios acerca del progreso en la resolución de problemas y errores.
Gestionar la continuidad
Definir la política de continuidad del negocio, objetivos y alcance. • Verificar que existan procesos de negocio internos y subcontratados y actividades de servicio que son críticas para las operaciones de la empresa o necesarias para cumplir con las obligaciones legales y/o contractuales. • Verificar la definición y documentación de objetivos y alcances mínimos acordados de la política de continuidad del negocio. • Verificar la identificación de procesos de soporte al negocio esenciales y servicios TI relacionados.
Mantener una estrategia de continuidad. • Verificar la realización de un estudio de análisis de impacto en el negocio • Verificar que se mantenga actualizado el plan de continuidad, manifestando la probabilidad de amenazas que puedan causar pérdidas e identificar medidas que puedan reducir la probabilidad y el impacto
Desarrollar e implementar una respuesta a la continuidad del negocio. • Verificar el desarrollo de planes de continuidad de negocio operativos que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio y/o planes temporales de proceso. • Verificar que los proveedores y socios externos clave tengan implantados planes de continuidad efectivos. • Verificar la definición y documentación de los recursos para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI.

Ejercitar, probar y revisar el plan de continuidad. • Verificar la definición los objetivos para ejercitar y probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio. • Verificar la implementación de pruebas del plan de continuidad asignando roles y responsabilidades para realizar ejercicios.
Revisar, mantener y mejorar el plan de continuidad. • Verificar que exista un plan y la capacidad de continuidad frente a la las posibilidades y los objetivos de negocio actuales, tanto estratégicos como operativos. • Verificar la aprobación de los cambios en la política, planes, procedimientos, infraestructura, roles y responsabilidades y la realización mediante un proceso de gestión de cambios. • Verificar la revisión regular del plan de continuidad para considerar el impacto de cambios nuevos o mayores en: organización de la empresa, procesos de negocio, acuerdos de externalización, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones.
Proporcionar formación en el plan de continuidad. • Verificar la definición y mantenimiento de los planes y requerimientos de planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes.
Gestionar acuerdos de respaldo. • Verificar que existan copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación. • Verificar que los sistemas, aplicaciones, datos y documentación mantenidos o procesados por terceras partes están adecuadamente respaldados o asegurados de otra forma. • Verificar que exista la difusión y la formación en Planes de Continuidad

de Negocio (BCP) y mantener legibles las copias de seguridad y las archivadas periódicamente.
Ejecutar revisiones postreanudación. • Verificar la efectividad del plan, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, resiliencia a incidentes, infraestructura técnica y estructuras organizativas y relaciones. Además identificar debilidades u omisiones en el plan y las capacidades y hacer recomendaciones para la mejora.
Gestionar servicios de seguridad
Proteger contra software malicioso (*malware*). • Verificar la instalación y activación de herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).
Gestionar la seguridad de la red y las conexiones. • Verificar la existencia de un análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones. • Verificar la realización de pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.
Gestionar la seguridad de los puestos de usuario final. • Verificar la configuración los sistemas operativos de forma segura. • Verificar la implementación de mecanismos de bloqueo de los dispositivos. • Verificar el cifrado de la información almacenada de acuerdo a su clasificación. • Verificar la gestión acceso y control remoto. • Verificar la gestión de la configuración de la red de forma segura. • Verificar la proteger la integridad del sistema.

• Verificar la protección física a los dispositivos de usuario final.
Gestionar la identidad del usuario y el acceso lógico. • Verificar la existencia de derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. • Verificar la administración de todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados. • Verificar la segregación y la gestión de cuentas de usuario privilegiadas.
Gestionar el acceso físico a los activos de TI. • Verificar el aseguramiento que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades. • Verificar el registro y supervisión todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.
Gestionar documentos sensibles y dispositivos de salida. • Verificar procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro, en y fuera de la empresa. • Verificar la asignación de privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio. • Verificar la existencia de procedimientos de destruir la información sensible para proteger dispositivos de salida (por ejemplo, desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para destruir formularios especiales y otros documentos confidenciales).
Supervisar la infraestructura para detectar eventos relacionados con la

seguridad. • Verificar el registro de los eventos relacionados con la seguridad reportada por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.
Gestionar los Controles de los Procesos del Negocio
Controlar el procesamiento de la información. • Verificar informes de control de procesamiento de la información.
Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización. • Verificar la asignación de los niveles de autoridad para la aprobación de transacciones, límites y cualquier otra decisión relativa a los procesos de negocio, basadas en los roles de trabajo aprobados. • Verificar la asignación de roles para las actividades sensibles de manera que haya una segregación clara de funciones. • Verificar la revisión periódica de las definiciones de control de acceso, registros e informes de excepciones para asegurar que todos los privilegios de acceso son válidos y están alineados con el personal actual y sus roles asignados.
Asegurar la trazabilidad de los eventos y responsabilidades de información. • Verificar la captura y/o eliminación de la fuente de información, evidencia que la soporta y el registro de las transacciones de acuerdo con la política de retención.
Asegurar los activos de información. • Verificar la aplicación de las políticas de clasificación de datos y uso aceptable y seguridad y los procedimientos para proteger los activos de información bajo el control del negocio. • Verificar la identificación e implementación de procesos, herramientas y

técnicas para verificar razonablemente el cumplimiento.

3.1.2.2.4 SUPERVISAR, EVALUAR Y VALORAR(MEA)

Supervisar, Evaluar y Valorar el Sistema de Control Interno
Supervisar el control interno. • Verificar la realización de actividades de evaluación y supervisión del control interno basadas en los estándares de gobierno organizativos y los marcos y prácticas aceptadas. • Verificar el mantenimiento del sistema de control interno de TI, considerando los cambios en curso en el negocio y el riesgo de TI, el entorno de control organizativo, los procesos de negocio y de TI relevantes y el riesgo de TI • Verificar la evaluación del rendimiento del marco de control de TI, realizando estudios comparativos con los estándares y buenas prácticas • Verificar la evaluación del estado de los controles internos de los proveedores externos de servicios y confirmar que dichos proveedores cumplen con los requisitos legales y regulatorios, así como las obligaciones.
Revisar la efectividad de los controles sobre los procesos de negocio • Verificar la identificación de controles clave y su validación. • Verificar el desarrollo e implementación de los procedimientos eficientes para determinar si la información está basada en los criterios de información.
Realizar autoevaluaciones de control. • Verificar la existencia de planes y alcances para identificar los criterios en la realización de las autoevaluaciones. Además asignar la responsabilidad de la autoevaluación a las personas oportunas con el fin de asegurar la objetividad y la competencia.

Identificar y comunicar las deficiencias de control. • Verificar la identificación, comunicación y registro de excepciones de los controles y asignar responsabilidad de su resolución y comunicación de los resultados.
Garantizar que los proveedores de aseguramiento son independientes y están cualificados. • Verificar los acuerdos, códigos de ética, estándares aplicables y estándares de aseguramiento, para establecer la independencia, competencia y cualificación de los proveedores de aseguramiento.

3.1.3 Definición de valores para evaluación

Cada uno de los elementos que forman parte de la evaluación debe tener una escala específica para su medición, es así, que para las prácticas de gestión y los atributos de proceso, los valores se reflejan en una escala discreta compuesta por los siguientes elementos:

No implementado – N-. Entre 0% y 15%. Hay muy poco o incluso ninguna evidencia de cumplimiento del atributo definido en el proceso evaluado.

Parcialmente Logrado – P - . Entre 16% y 50%. Hay evidencia de alguna aproximación, y algún logro, al cumplimiento del atributo en el proceso evaluado. Algunos aspectos del cumplimiento del atributo pueden ser impredecibles.

Ampliamente logrado - L -. Entre 51% y 85%. Hay evidencias de una aproximación sistemática, y logro significativo, al cumplimento del atributo en el proceso evaluado. La ejecución del proceso puede variar en algunas áreas o unidades de trabajo.

Totalmente logrado- F . Entre 86% y 100 %. Hay evidencias de una completa y sistemática aproximación, y logro total, al cumplimiento del atributo en el proceso evaluado. No hay debilidades significativas en las unidades de trabajo.

El valor para utilizar en la calificación se obtiene de encontrar el promedio de los valores porcentuales de sus prácticas de gestión, de esta manera, como se puede observar en la Ecuacion1.

$$\boldsymbol{Valor} = \frac{\%\ Limite\ Inferior + \%Limite\ Superior}{2}$$

Ecuación 1: Valores de Evaluación

Cabe indicar que para la escala de N – No se ha alcanzado, no se aplica la formula, ya que el promedio calculado se acerca al valor de 0, para las otras escalas los valores alcanzados son los que se muestran en la Tabla 7: Definición de valores para calificación.

Escala	Valor
N - No se ha alcanzado	0
P - Parcialmente logrado	0.33
L – Ampliamente logrado	0.67
F - Totalmente logrado	1

Tabla 7: Definición de valores para calificación

3.1.4 Definición de la medida de evaluación de la capacidad de los procesos.

3.1.4.1 Capacidad Nivel 1

Los indicadores a nivel de capacidad 1 son específicos para cada proceso y se utilizan para determinar si el siguiente nivel ha sido alcanzado.

Todos los procesos definidos en el marco de referencia Cobit 5 tienen la misma estructura, por lo tanto a partir de definir las métricas para este proceso se puede construir las métricas de los demás procesos del modelo de referencia.

Los procesos están compuestos de cinco elementos fundamentales, definidos en el documento de (Isaca - Cobit 5, 1013):

1. El propósito del proceso,
2. Los resultados o metas para la implementación exitosa del proceso,
3. Las prácticas de gestión , que ejecutan tareas y/o actividades para generar un resultado,
4. Entradas, que son productos de trabajo que están relacionadas con los resultados, y a través de estos con las prácticas base.
5. Salidas, que son productos de trabajo que están relacionadas con los resultados, y que son indicadores para observar que el proceso cumple el propósito.

A continuación se muestra una figura con la referencia de los elementos descritos:

Process ID	EDM02		
Process Name	Ensure Benefits Delivery		
Process Description	Optimise the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs.		
Process Purpose Statement	Secure optimal value from IT-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.		
Outcomes (Os)			
Number	**Description**		
EDM02-O1	The enterprise is securing optimal value from its portfolio of approved IT-enabled initiatives, services and assets.		
EDM02-O2	Optimal value is derived from IT investment through effective value management practices in the enterprise.		
EDM02-O3	Individual IT-enabled investments contribute optimal value.		
Base Practices (BPs)			
Number	**Description**		**Supports**
EDM02-BP1	**Evaluate value optimisation.** Continually evaluate the portfolio of IT-enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgement on any changes in direction that need to be given to management to optimise value creation.		EDM02-O1
EDM02-BP2	**Direct value optimisation.** Direct value management principles and practices to enable optimal value realisation from IT-enabled investments throughout their full economic life cycle.		EDM02-O2
EDM02-BP3	**Monitor value optimisation.** Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions.		EDM02-O3
Work Products (WPs)			
Inputs			
Number	**Description**		**Supports**
APO02-WP12	Strategic road map		EDM02-BP1 EDM02-O1
APO05-WP5	Investment return expectations		
APO05-WP8	Selected programmes with return on investment (ROI) milestones		
APO05-WP11	Benefit results and related communications		
BAI01-WP13	Stage-gate review results		
APO05-WP9	Investment portfolio performance reports		EDM02-BP3 EDM02-O3
Outputs			
Number	**Description**	**Input to**	**Supports**
EDM02-WP1	Evaluation of strategic alignment	APO02.04 APO05.03	EDM02-BP1 EDM02-O1
EDM02-WP2	Evaluation of investment and services portfolios	APO05.03 APO05.04 APO06.02	
EDM02-WP3	Investment types and criteria	APO05.01 APO05.03	
EDM02-WP4	Requirements for stage-gate reviews	BAI01.01	
EDM02-WP5	Feedback on portfolio and programme performance	APO05.04 APO06.05 BAI01.06	
EDM02-WP6	Actions to improve value delivery	EDM05.01 APO05.04 APO06.02 BAI01.01	

Figura 10: Esquema de definición de los procesos **(Isaca - Cobit 5, 1013)**

Es importante resaltar que cada uno de los productos de trabajo tanto de entrada y salida está asociado a los resultados del proceso.

3.1.4.1.1 Definición de la métrica

Las métricas del nivel 1 han sido definidas con el objetivo de valorar la capacidad de un proceso, en relación con un proceso definido por un modelo de evaluación, para nuestro caso la fuente es el marco de referencia COBIT 5.

Para el caso propuesto se utilizarán como componente principal la evaluación de las prácticas base, que apoyan el resultado de los procesos.

A continuación se presenta la forma de realizar la valoración de la capacidad de los procesos:

Métrica	Definición
NM	Número de metas del proceso a evaluar.
NPG	Número de prácticas de gestión del proceso a evaluar.
NPGMi	Número de prácticas gestión que contribuyen al logro de la meta i, del proceso a evaluar.
PM	Peso de cada uno de los metas del proceso a evaluar. $$PM = \frac{1}{NM}$$
VPGi	Valor de las prácticas gestión para la meta **i**, realizadas o llevadas a cabo por la organización (*).
GCMi (PG)	Grado de cumplimiento de la meta **i**, en función de las prácticas de gestión. $$GCMi(PG) = \frac{VPGi}{NPGMi}$$
CP (PG)	Medida de capacidad del proceso en función de las prácticas gestión. $$CP\ (PG) = PM * \sum_{i}^{n} GCMi\ (PG)$$

Tabla 8: Definición de Métricas, Evaluación procesos Nivel 1

- El valor de la métrica **VPGi** se obtiene de sumar el **valor del grado de realización de las prácticas de gestión** que contribuyen al logro de la meta **i**.

El **valor del grado de realización de una práctica base o meta** se obtiene del promedio del **valor del grado de ejecución de las actividades** que forman la práctica base.

Cada actividad tiene un grado de realización al cual se le asigna un valor según lo definido en la Tabla 7: Definición de valores para calificar.

Los productos de trabajo sirven como herramienta de apoyo para determinar el cumplimiento de las prácticas base y deben ser tomados en cuenta durante la aplicación de la evaluación, como referencia se puede utilizar el documento *Process Assessment Model Cobit 5* (Isaca - Cobit 5, 1013).

3.1.4.1.2 Formulario de recolección de información

Para obtener el **VPGi** (valor de las prácticas base para el resultado i, realizadas o llevadas a cabo por la organización), se ha preparado un formulario de recolección de información por cada uno de los procesos que se desean evaluar.

APO01	**Gestionar el Marco de Gestión de TI**						
		EVALUACION					
METAS		**N**	**P**	**L**	**F**	**CP**	**Observaciones**
M1	Se ha definido y se mantiene un conjunto eficaz de políticas.	0				0	
M2	Todos tienen conocimiento de las políticas y de cómo deberían implementarse.	0					
		EVALUACION					
APO01.01	**Definir la estructura organizativa.**	**N**	**P**	**L**	**F**	**VP**	**Observaciones**

						G	
M1	Verificar que se establezca el alcance, las funciones internas y externas, los roles internos y externos, las capacidades y los derechos incluidas las actividades de TI					0	
	Verificar el alineamiento de la organización relativa a TI con los modelos organizativos de arquitectura corporativa (Plan TI).						
	Verificar que exista un comité estratégico y directivo de TI a fin de revisar, supervisar y realizar seguimiento las inversiones, los niveles de servicio y las mejoras en el servicio.						
APO01.02	**Establecer roles y responsabilidades.**	**N**	**P**	**L**	**F**	**VPG**	**Observaciones**
M1	Verificar que los roles y responsabilidades estén estructurados de acuerdo a las necesidades y objetivos de organización, a fin de delimitar claramente las responsabilidades y la rendición de cuentas, especialmente para la aprobación y toma de decisiones.					0	
	Verificar que se incluya en las descripción de roles y responsabilidades, la adhesión a las políticas y los procedimientos de gestión, al código ético y a las prácticas profesionales.						
	Verificar que los roles y responsabilidades sean difundidas a todos los empleados de la organización.						
APO01.06	**Definir la propiedad de la información (datos) y del sistema.**	**N**	**P**	**L**	**F**	**VPG**	**Observaciones**
M1	Verificar que existan políticas y directrices para asegurar la adecuada clasificación de la información en la organización.					0	
	Verificar que se cree o se mantenga un inventario de la información incluyendo un listado de los propietarios, custodios y clasificaciones. Incluir los sistemas subcontratados y aquellos cuya propiedad debe permanecer dentro de la empresa.						
	Verificar la implementación de procedimientos para asegurar la integridad y consistencia de la información almacenada en formato electrónico.						
APO01.08	**Mantener el cumplimiento con las políticas y procedimientos.**	**N**	**P**	**L**	**F**	**VPG**	**Observaciones**
M2	Verificar que exista un seguimiento del cumplimiento de las políticas y procedimientos.					0	
	Verificar que se analice las tendencias en el funcionamiento y cumplimiento para adoptar las acciones apropiadas.						

Tabla 9: Formulario de recolección de información Nivel 1

Los componentes principales son los resultados del proceso (Metas), en conjunto con sus prácticas base (Prácticas de gestión) y las actividades que las apoyan.

3.1.4.2 Niveles de capacidad de 2 a 5

En contraste con el nivel de capacidad 1, las evaluaciones de los niveles de capacidad de 2 a 5 se basan en indicadores genéricos de procesos, por lo tanto para definir las métricas desde el nivel 2 hasta el nivel 5 se lo puede realizar de tal manera que sea aplicado de forma similar sin ninguna modificación.

A continuación se presenta una breve descripción para estos niveles de capacidad:

- Una práctica genérica es una actividad de gestión que realza la capacidad para realizar un proceso. Una práctica genérica soporta la implementación o gestión y puede ser aplicada a cualquier proceso. Las prácticas genéricas permiten su medición individual para así determinar el grado de alcance del atributo al que pertenecen y el nivel en que se encuentra el proceso en estudio.

- Los indicadores del producto de trabajo genérico (GWP) son conjuntos de características que se espera que sean evidentes en los productos del trabajo de tipo genérico como resultado del logro de un atributo. Los productos genéricos del trabajo forman la base para la clasificación de los productos de trabajo definidos como indicadores del funcionamiento del proceso; representan los tipos básicos de productos de trabajo que pueden ser entradas o salidas de todos los tipos de proceso.

3.1.4.2.1 Definición de la métrica

De acuerdo al marco de referencia COBIT 5 basado en la norma ISO/IEC15504, la capacidad de un proceso se puede medir por la implementación exitosa de sus atributos de proceso, los atributos de proceso se pueden medir por la implementación exitosa de sus resultados, a su vez los resultados están relacionados con prácticas genéricas y productos de trabajo genéricos.

A continuación se presenta la forma de realizar la valoración de la capacidad de los procesos:

Métricas del atributo del proceso	
Métrica	**Definición**
NAT	Número de atributos del proceso a evaluar definidos.
NPG	Número de prácticas genéricas del atributo del proceso a evaluar.
NPATi	Número de prácticas genéricas que contribuyen al logro del resultado del atributo i, del proceso a evaluar.
PAT	Peso de cada uno de los resultados del atributo del proceso a evaluar. $$PAT = \frac{1}{NAT}$$
VPGNi	Valor de las prácticas genéricas para el resultado i, realizadas o llevadas a cabo por la organización (*)
GCRi (PG) Grado de cumplimiento del resultado i, en función de las prácticas base.	Es el promedio del valor de las practicas genéricas para el resultado *i* $$GCRi\ (PG) = \frac{VPGNi}{NPATi}$$

MCAT (PG)	Medida de cumplimiento del atributo del proceso en función de las prácticas genéricas. $$MCAP\ (PG) = \text{PAT} * \sum_{i}^{n} GCRi\ (PG)$$

Tabla 10: Definición de Métricas, Evaluación procesos Nivel 2 al 5

Para obtener **VPGNi,** hay que tomar en cuenta la calificación asignada a cada una de las prácticas genéricas de acuerdo a los valores definidos en la Tabla 10, de donde la sumatoria de esta calificación definirá el valor final.

3.1.4.2.2 Formulario de recolección de información

Para obtener el **VPGNi** (valor de las prácticas genéricas para el resultado i, realizadas o llevadas a cabo por la organización), se ha preparado un formulario de recolección de información por cada uno de los procesos y atributos que se desean evaluar.

DOMINIO	**Alinear, Planificar y Organizar (APO)**						
APO01	**Gestionar el Marco de Gestión de TI**						
NIVEL 2		**N**	**P**	**L**	**F**	**CAP**	**Obser**
		EVALUACION					
NIVEL 2.1	**Gestión del desempeño**	**N**	**P**	**L**	**F**	**VPGN**	**Obser**
	Los objetivos para el desempeño de los procesos están identificados						
	El desempeño de los procesos es planeado y monitoreado						
	El desempeño de los procesos es ajustado para cumplir con los planes.						
	Las autoridades y responsables del desempeño de los procesos están definidos, asignados y comunicados.						

	Los recursos y la información necesaria para el desempeño de los procesos están identificados, puestos a disposición, asignados y utilizados.						
	Las interfaces están gestionadas para asegurar que la comunicación y la asignación de responsabilidades sea eficaz y clara						

		EVALUACION					
NIVEL 2.2	**Gestión del producto de trabajo**	**N**	**P**	**L**	**F**	**VPGN**	**Obser**
	Los requisitos para los productos de trabajo del proceso están definidos						
	Los requisitos de la documentación y control de los productos de trabajo están definidos.						
	Los productos de trabajo están debidamente identificados, documentados y controlados.						
	Los productos de trabajo están revisados de acuerdo con planes previstos y se ajustan para cumplir los requerimientos.						

NIVEL 3		**N**	**P**	**L**	**F**	**CAP**	**Obser**
		EVALUACION					
NIVEL 3.1	**Definición de procesos**	**N**	**P**	**L**	**F**	**VPGN**	**Obser**
	Un proceso estándar, incluyendo la adecuada adaptación de las guías, esto define que describen los elementos, fundamentalmente los que deben ser incorporados a un proceso definido.						
	La secuencia y la interacción del proceso estándar con otros procesos esta determinado.						
	Las competencias y roles para llevar a cabo los procesos están definidos como parte de los procesos estándar.						
	La infraestructura y el entorno de trabajo están identificados como parte de los procesos estándar.						
	Métodos para el seguimiento de la eficacia y adecuación del proceso están determinados.						

		EVALUACION					
NIVEL 3.2	**Implementación de procesos**	**N**	**P**	**L**	**F**	**VPGN**	**Obser**
	Un proceso definido se implementa sobre la base de un proceso estándar seleccionado y / o adaptado apropiadamente.						
	Los roles, responsabilidades y autoridades para realizar						

	los procesos están asignados y comunicados						
	El personal que realiza la definición de procesos son competentes sobre la base de una educación adecuada, capacitación y experiencia.						
	Los recursos y la información necesaria para realizar el proceso están disponibles, asignados y utilizados.						
	La infraestructura y el entorno de trabajo para la definición de procesos está disponible, administrada y mantenida.						
	Los datos apropiados están almacenados y analizados como una base para entender el comportamiento y demostrar la identidad y la eficacia del proceso y evaluar el donde mejorar la continuidad del proceso.						

NIVEL 4	**N**	**P**	**L**	**F**	**CAP**	**Obser**

		EVALUACION					
NIVEL 4.1	**Medición de procesos**	**N**	**P**	**L**	**F**	**VPGN**	**Obser**
	Necesidades de información de proceso en apoyo de los objetivos de negocio definidos están establecidas.						
	Los objetivos de medición del proceso derivan de las necesidades de información.						
	Los objetivos son cuantitativos para el desempeño del proceso en apoyo de los objetivos de negocio						
	Las medidas y frecuencia de las mediciones se identifican y se definen de acuerdo con los objetivos de medición de procesos y objetivos cuantitativos para el desempeño del proceso.						
	Los resultados de la medición se recogen, se analizaron e informaron a fin de vigilar el grado en que se cumplen los objetivos cuantitativos del desempeño del proceso.						
	Los resultados de medición se utilizan para caracterizar el desempeño del proceso.						

		EVALUACION					
NIVEL 4.2	**Control de procesos**	**N**	**P**	**L**	**F**	**VPGN**	**Obser**
	Las técnicas de análisis y control se determinan y aplican en su caso.						
	Los límites de control de la variación se establecen para la ejecución normal del proceso.						
	Los datos de medición analizan las causas especiales de variación.						

	Se toman las acciones correctivas para hacer frente a las causas especiales de variación.						
	Los límites de control se restablecen (cuando sea necesario) después de la acción correctiva.						

NIVEL 5		N	P	L	F	CAP	Obser
		EVALUACION					
NIVEL 5.1	**Innovación de procesos**	**N**	**P**	**L**	**F**	**VPGN**	**Obser**
	Los objetivos de mejora de procesos se definen para apoyar los objetivos de negocio relevantes.						
	Los datos apropiados son analizados para identificar las causas comunes de las variaciones en el desempeño del proceso.						
	Los datos apropiados son analizados para identificar las oportunidades de mejores prácticas y la innovación.						
	Identificación de oportunidades de mejora derivados de las nuevas tecnologías y conceptos de proceso.						
	Una estrategia de implementación es establecida para alcanzar los objetivos de mejora de procesos.						

		EVALUACION					
NIVEL 5.2	**Optimización de procesos**	**N**	**P**	**L**	**F**	**VPGN**	**Obser**
	El impacto de los cambios propuestos se evalúa con los objetivos del proceso definido y el proceso estándar.						
	La implementación de todos los cambios acordados es administrada para asegurar que cualquier interrupción en el desempeño de los procesos sea entendida y se actúe en consecuencia.						
	En base a los resultados reales, la eficacia del cambio de proceso se evalúa con los requisitos de los productos definidos y objetivos del proceso para determinar si los resultados se deben a causas comunes o especiales.						

Tabla 11: Formulario de recolección de información Niveles del 2 al 5

3.1.5 Definición de los niveles de capacidad

El nivel de capacidad de un proceso depende de si los atributos del proceso a ese nivel han sido alcanzados en gran medida (L) y totalmente (F) o si los atributos de proceso para los niveles más bajos se han alcanzado totalmente (F). La tabla 12 presentada a continuación, muestra cada nivel y las calificaciones necesarias que cada uno debe alcanzar.

Nivel de Capacidad	Atributos del proceso	Grado de cumplimiento esperado
Nivel 1. Alcanzado	Realización del proceso	L o F
Nivel 2. Gestionado	Realización del proceso	F
	Gestión de la realización	L o F
	Gestión de los productos	L o F
Nivel 3. Establecido	Realización del proceso	F
	Gestión de la realización	F
	Gestión de los productos	F
	Definición del proceso	L o F
	Desarrollo del proceso	L o F
Nivel 4. Predecible	Realización del proceso	F
	Gestión de la realización	F
	Gestión de los productos	F
	Definición del proceso	F
	Desarrollo del proceso	F
	Medición de procesos	L o F
	Control del proceso.	L o F
Nivel 5. Optimizado	Realización del proceso	F

	Gestión de la realización	F
	Gestión de los productos	F
	Definición del proceso	F
	Desarrollo del proceso	F
	Medición de procesos	F
	Control del proceso.	F
	Innovación del proceso	L o F
	Optimización del proceso	L o F

Tabla 12: Definición de los Niveles de Capacidad

Después de realizada la evaluación se verificará el nivel para determinar la capacidad por cada uno de los procesos en la organización.

3.1.6 Determinación de categorías por grados de madurez de los procesos.

3.1.6.1 Determinación del nivel de madurez

Para la evaluación del nivel de madurez de la organización o nivel de madurez resultado de la evaluación se tienen en cuenta los resultados de la evaluación de los procesos asociados y definidos por el modelo de referencia.

De donde, si todos los procesos evaluados se hallan en un nivel de capacidad **N**, entonces se puede determinar que la organización ha alcanzado el grado de madurez N, según la correlación de equivalencias definida para los niveles de capacidad y los niveles de madurez como parte del presente modelo:

NIVEL DE MADUREZ	DESCRIPCIÓN
Nivel de madurez 0	La organización no tiene una implementación efectiva de los procesos
Nivel de madurez 1	Algunos de los procesos objeto de evaluación alcanzan el nivel de capacidad 1, es decir, existen productos resultantes para los mismos y el proceso se puede identificar.
Nivel de madurez 2	Los procesos objeto de evaluación tienen el nivel de capacidad 2 o superior.
Nivel de madurez 3	Los procesos objeto de evaluación tienen el nivel de capacidad 3 o superior.
Nivel de madurez 4	Uno o más procesos tienen nivel de capacidad 4 o superior.
Nivel de madurez 5	Uno o más procesos tienen nivel de capacidad 5.

Tabla 13: Definición del nivel de madurez de una organización.

3.1.7 Generación de plantillas para la aplicación del modelo de madurez.

3.1.7.1 Generación de Plantillas para Nivel 1

El detalle de las plantillas desarrolladas para la evaluación de la capacidad de los procesos a nivel 1, se encuentran en el Anexo 1.

3.1.7.2 Generación de Plantillas para Niveles del 2 al 5.

El detalle de las plantillas desarrolladas para la evaluación de la capacidad de los procesos en los niveles 2 a 5, se encuentran en el Anexo 2.

CAPITULO IV

4.1 Aplicación del modelo de madurez

4.1.1 Planificación y metodología para aplicar la propuesta.

Para la aplicación de la propuesta ~~dentro~~ de las organizaciones se plantea una estrategia procedimental de 4 fases, de esta manera:

- **Fase 1.- Preparar la Evaluación.**

  1. Definir el caso de estudio.
  2. Identificar los interlocutores de acuerdo a las responsabilidades asignadas dentro de la organización.
  3. Identificar las fuentes de información válidas (aplicaciones, bitácoras, portales, etc.)
  4. Definir el calendario de entrevistas con los interlocutores.

- **Fase 2.- Recabar información y aplicar el Modelo**

  1. Preparar la entrevista.
  3. Ejecutar la entrevista.
     - Llenar la plantilla de madurez de cada proceso en Nivel 1.
     - Llenar la plantilla de madurez de cada proceso en Niveles del 2 al 5
  4. Analizar la entrevista

- **Fase 3.- Analizar la información.**

  1. Analizar cada elemento de información en las plantillas.
  2. Generar la plantilla de evaluación general.

- **Fase 4.- Formular las conclusiones**

1. Analizar el nivel de madurez.
2. Desarrollar un informe con las conclusiones.

4.1.2 Determinación del grado de capacidad de los procesos en una organización

- **Proceso**

Fase 1.- Preparar la Evaluación.

1. Definición del caso de estudio.- A fin de probar el modelo, la SEPS realizó un acercamiento con la Cooperativa de Ahorro y Crédito "Textil 14 de Marzo", para ejecutar la evaluación de su nivel de madurez.

2. Identificar los interlocutores de acuerdo a las responsabilidades asignadas dentro de la organización.- Dentro de la institución designada se precisó como interlocutor principal a la persona encargada de la Dirección de Sistemas, con quien se llevó a cabo la coordinación, planificación y aplicación del modelo.

3. Identificar las fuentes de información válidas (aplicaciones, bitácoras, portales, etc.)

Las fuentes de información evaluadas dentro de la institución fueron las siguientes:

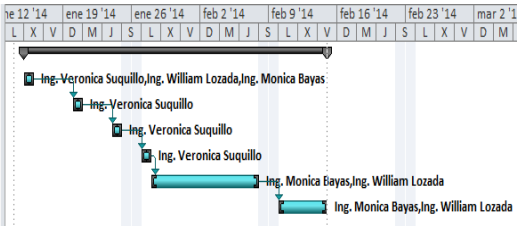
- Bases de Datos.
- Controles de seguridad física y lógica.
- Equipos informáticos.
- Aplicaciones.

- Hardware,
- Software,
- Manuales, procedimientos y políticas
- Registros de bitácoras.

4. Definir el calendario de entrevistas con los interlocutores.

Para la aplicación del modelo se planificaron entrevistas con los encargados de las diferentes áreas involucradas, según se detalla en el siguiente cronograma:

Nombre de tarea	Duración	Comienzo	Fin
Modelo de Madurez - Cooperativa	**23 días**	**mié 1/15/14**	**vie 2/14/14**
Elaboración del Cronograma	1 día	mié 1/15/14	mié 1/15/14
Reunión 1	1 día	lun 1/20/14	lun 1/20/14
Reunión 2	1 día	vie 1/24/14	vie 1/24/14
Reunión 3	1 día	lun 1/27/14	lun 1/27/14
Análisis de Resultados	9 días	mar 1/28/14	vie 2/7/14
Categorización y Elaboración del Informe	5 días	lun 2/10/14	vie 2/14/14



Fase 2.- Recabar información y aplicar el Modelo

1. Preparar la entrevista.

La preparación de la entrevista tuvo como propósito principal la revisión de las plantillas de evaluación de los niveles de capacidad de los procesos.

2. Ejecutar la entrevista.

- Llenar la plantilla de nivel de capacidad de cada proceso en Nivel El proceso de evaluación se ejecutó con el llenado de plantillas de las matrices para los procesos en Nivel 1.

- Llenar la plantilla de nivel de capacidad en cada proceso en Niveles del 2 al 5

De acuerdo a la metodología utilizada, únicamente si los procesos en su nivel de evaluación se hallan alcanzados totalmente (F), se efectuará la evaluación en el nivel siguiente, sin embargo de acuerdo a los resultados obtenidos este requisito no fue alcanzado, por lo que la evaluación finalizo con la calificación de la capacidad de los procesos en nivel 1 para la organización.

2. Analizar la entrevista

Después de la ejecución de las entrevistas se evaluaron los resultados preliminares para determinar la pertinencia de la planificación de una segunda ronda de entrevistas que permita evaluar los procesos en los niveles 2 a 5, de donde se concluyó que la organización al momento de la ejecución del presente trabajo no cumplía con los requisitos necesarios para realizar la evaluación a estos niveles.

Fase 3.- Analizar la información.

1. Generar la plantilla de evaluación general y específicas
2. Generar el informe de evaluación de acuerdo a los resultados obtenidos en el examen general.

El informe de evaluación general se presenta como un insumo independiente en el apartado 4.1.3.

4.1.3 Informe de Evaluación

1. Título

Aplicación de una prueba piloto del modelo de madurez tecnológico en la Cooperativa de Ahorro y Credito "Textil 14 de Marzo".

2. Objetivo

- Realizar una prueba piloto del Modelo de madurez tecnológico desarrollado en base a COBIT 5 para categorizar a las Instituciones Financieras, de los segmentos 3 y 4 de la SEPS, mediante la evaluación del nivel de capacidad de procesos de la Cooperativa de Ahorro y Crédito "Textil 14 de Marzo", para determinar la aplicabilidad y robustez del modelo, identificar las debilidades y generar recomendaciones para mejorarlo.

3. Alcance

El despliegue de la prueba piloto de este modelo fue realizado en la oficina Matriz de la Cooperativa de Ahorro y Crédito "Textil 14 de Marzo", ubicada en la Parroquia San Rafael, cantón Rumiñahui en la Provincia de Pichincha, clasificada como una organización perteneciente al segmento 3 según la clasificación de las organizaciones controladas por la Superintendencia de Economía Popular y Solidaria, en el período comprendido entre los meses de enero y febrero del año 2014.

4. Metodología utilizada

La metodología empleada para la definición del modelo de madurez tecnológica de las organizaciones fue planteada tomado en cuenta la definición de procesos de

tecnología del marco de referencia ampliamente reconocido COBIT 5, que para su evaluación utiliza el enfoque de la capacidad de los procesos basado en la norma internacional ISO/IEC 15504-2, además se utilizó como insumo la guía denominada *Process Assessment Model* preparada por ISACA para la ejecución del proceso de evaluación de capacidad de procesos.

5. Antecedentes

- **Breve reseña**

La Cooperativa de Ahorro y Crédito "TEXTIL 14 DE MARZO" , nace en el año 1968 en San Rafael Valle de los Chillos, impulsada por los obreros de la fábrica "Indutex", es constituida como una organización paralela al Comité de Empresa de la fábrica luego de un proceso de capacitación realizado por el Instituto Sindical INESE.

En el inicio, solamente podían pertenecer a la cooperativa los empleados de la fábrica y su avance estuvo ligado al crecimiento de la misma. Hasta el año de 1991 solo se contaba con el gerente y se atendía solamente a los obreros de Indutex, de la Textiles Nacionales y de Textiles Durero, posteriormente se contratan dos empleados quienes eran los encargados de realizar todos los trámites correspondientes.

En la asamblea general de socios del 20 de julio de 1996 luego de un informe favorable y por convenir al desarrollo de la COAC. TEXTIL 14 DE MARZO se solicita que la Cooperativa se declare como "abierta". Es aprobada y ratificada la decisión por unanimidad de los 110 socios existentes para ese entonces y se pide se proceda a la reforma del estatuto.

- **Misión**

La misión de la Cooperativa es:" Atender a nuestros socios con servicios de calidad, eficiencia administrativa e ideas innovadoras.

Apoyaremos sus iniciativas a partir de un equipo de trabajo efectivo, una administración responsable y un Cuerpo Directivo comprometido con el crecimiento y solidez de la cooperativa."

- **Visión**

La visión de la Cooperativa es:" Ser una cooperativa de prestigio en el sector financiero, reconocida por su solidez, rentabilidad, cobertura de servicios, que cuenta con personal capacitado y comprometido, procesos eficientes, tecnología de punta y capacidad institucional para responder a la confianza de sus socios."

- **Alcance geográfico**

En la actualidad la Cooperativa tiene su oficina matriz en la parroquia San Rafael, perteneciente al cantón Rumiñahui en la Provincia de Pichincha, además posee 10 sucursales distribuidas en varias sectores dentro de la provincia como: Conocoto, El Inca, El Arenal, Amaguaña, Machachi, Guamaní, La Biloxi, El Camal, Santo Tomás, así como también la agencia Santo Domingo ubicada en la provincia de Santo Domingo de los Tsáchilas.

6. Observaciones para la organización

Después de la ejecución de la prueba piloto se identificó la idoneidad de la aplicación del modelo a través de los resultado obtenidos, pues estos dieron paso al

planteamiento de observaciones a la capacidad de los procesos evaluados dentro de la organización, para los que se ha preparado el análisis respectivo y la recomendaciones con el fin de generar una retroalimentación que sea beneficiosa y aporte al crecimiento de la organización, de esta manera:

APO01 Gestionar el marco de gestión de TI.

- **La gestión del marco de TI, evidencia debilidades respecto a la visión general de la organización.**

La estructura orgánica dentro de la organización no responde a un modelo donde se involucre directamente al área de TI como un ente agregador de valor.

Se han definido roles dentro de la organización, sin embargo no se han delimitado de manera clara y precisa las responsabilidades para la toma de decisiones y ejecución de procesos críticos.

La definición de la propiedad de la información es un tema pendiente a realizar dentro de la organización.

Existen políticas y procedimientos definidos de forma aislada, que no han sido vistos como un instrumento integral en el que se se sostenga la gestión de TI y la gestión de la organización como tal.

De acuerdo con el modelo desarrollado en base al marco de referencia COBIT 5.0, en la práctica de gestión APO01.01, se menciona que dentro de la organización se debe: “Establecer una estructura organizativa interna y extensa que refleje las necesidades del negocio y las prioridades de TI. Implementar las estructuras de

gestión requeridas (p. ej., comités) para permitir que la toma de decisiones se lleve a cabo de la forma más eficaz y eficiente posible."

De la misma manera para la práctica de gestión APO01.02, se busca "Establecer, acordar y comunicar roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades en las TI corporativas, que reflejen claramente las necesidades generales del negocio y los objetivos de TI, así como la autoridad, las responsabilidades y la rendición de cuentas del personal relevante."

En el caso de la práctica de gestión APO01.06, se busca "Definir y mantener las responsabilidades de la propiedad de la información (datos) y los sistemas de información.

Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación."

Según la práctica de gestión APO01.08 la organización está llamada a "Poner en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Seguir las tendencias y el rendimiento y considerarlos en el diseño futuro y la mejora del marco de control."

La visión del negocio se ha centrado en la gestión operativa, a través de la masificación de servicios, captación de nuevos clientes, expansión de su territorio de cobertura, entre otros, pero no se ha alineando con temas sensibles para fortalecer

una estrategia organizativa descuidando el crecimiento de áreas que podrían aportar de mejor manera al desarrollo integral de la organización.

Las principales consecuencias identificadas son: el incumplimiento de normativa legal, la apertura de brechas de seguridad que comprometan los principios de confidencialidad de la información, inconvenientes en la entrega de los servicios de tecnología que pueden llegar incluso a la indisponibilidad.

RECOMENDACIÓN 1

Ejecutar un proceso de evaluación de la estructura organizativa que permita involucrar al área de TI con la gestión de los objetivos estratégicos propuestos para el negocio.

RECOMENDACIÓN 2

Levantar y difundir dentro de la organización el manual de funciones definiendo de forma clara y precisa la responsabilidad y funciones a desempeñar por parte del personal de TI, respecto a las otras áreas dentro de la organización

RECOMENDACIÓN 3

Desarrollar y difundir políticas, directrices y procedimientos que permitan realizar una adecuada clasificación de la información, su administración, garantizando la responsabilidad frente a terceros.

RECOMENDACIÓN 4

Realizar un seguimiento continuo de la implementación y cumplimiento de las políticas, normas y procedimientos dentro de la organización, con el fin ejecutar las acciones correctivas en el momento adecuado.

APO02 Gestionar la estrategia.

- **La organización no cuenta con un diagnostico que permita identificar la capacidad actual de los recursos de TI, sus riesgos potenciales y el aporte que pudiera brindar para el crecimiento del negocio.**

El crecimiento de la organización ha estado dirigido por la adaptación del negocio al mercado y la respuesta de sus clientes a la oferta, sin embargo de la misma manera la evaluación de la capacidad y la gestión de los riesgos a los que se puede someter el área Tecnológica se lo ha manejado de forma poco planificada dependiendo del crecimiento periódico sin llegar a realizar un análisis profundo de la situación real de la organización.

No se ha identificado un plan estratégico para el área de TI, ni la relación entre el cumplimiento de objetivos de Ti con su grado de impacto de acuerdo al plan estratégico de la organización.

De acuerdo a lo esperado para la práctica de gestión APO02.05, dentro del marco de referencia COBIT 5, “Crear un plan estratégico que defina, en cooperación con las partes interesadas más relevantes, cómo los objetivos de TI contribuirán a los objetivos estratégicos de la empresa. Incluyendo cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, servicios y activos de TI. Orientar

las tecnologías para definir las iniciativas que se requieren para cerrar las diferencias, la estrategia de abastecimiento y las medidas que se utilizarán para supervisar el logro de los objetivos, para dar prioridad a las iniciativas y combinarlas en una hoja de ruta a alto nivel."

En la práctica de gestión APO02.02, se busca "Evaluar el rendimiento del negocio interno actual y las capacidades de TI y los servicios externos de TI para desarrollar un entendimiento de la arquitectura empresarial en relación con TI. Identificar los problemas que se están experimentando y generar recomendaciones en las áreas que pueden beneficiarse de estas mejoras. Considerar los aspectos diferenciadores y las opciones de proveedores de servicios y el impacto financiero, los costes y los beneficios potenciales de utilizar servicios externos."

El papel secundario que ha desarrollado el área de Ti dentro de la organización al ser considerada un área de apoyo llamada a solucionar inconvenientes.

Una de las principales consecuencias que puede llegar a sufrir la organización es rebasar la capacidad de su infraestructura y servicios de tecnología, con impacto en la operatividad del negocio, el servicio a los clientes y esto traducirse en pérdidas económicas que deberían ser calculadas en términos monetarios para ser presentados al negocio.

RECOMENDACIÓN 6

Realizar un análisis integral que permita identificar los problemas, fortalezas, oportunidades y amenazas en el entorno de TI de la organización, así como los

servicios puestos a disposición de las áreas de negocio, para determinar la capacidad actual y evaluar un crecimiento para atender necesidades futuras.

RECOMENDACIÓN 7

Establecer de forma explícita dentro de los planes de Tecnología el grado de apoyo al cumplimiento de los objetivos organizacionales establecidos dentro de la planificación estratégica a través de resultados medibles y cuantificables, que sean conocidos y aprobados por la alta gerencia dentro de la organización.

APO05 Gestionar el portafolio

- **El análisis y priorización para la inversión en proyectos de TI responde al planteamiento del plan operativo anual desarrollado por las áreas.**

La prioridad y decisión final para la ejecución de proyectos se halla bajo responsabilidad de la alta gerencia desde donde se evalúa la asignación del presupuesto, conforme al plan operativo enviado por cada una de las áreas.

Los proyectos planteados no contienen un componente de alineamiento estratégico que incluya los beneficios corporativos y el tratamiento del riesgo que permita mantener la disponibilidad de los recursos de financiamiento.

De acuerdo a la práctica de gestión APO05.03, se busca “Basado en los requisitos de la mezcla general del portafolio de inversión, evaluar y priorizar casos de negocio de programas y decidir sobre las propuestas de inversión. Dedicar fondos e iniciar los programas.”

Para la práctica de gestión APO05.05, el objetivo está dado por: “Mantener los portafolios de programas y proyectos de inversión, servicios de TI y activos de TI.”

Dentro de la organización no se ha establecido una metodología técnica para la priorización de proyectos que permita el análisis general y el grado de apoyo a los objetivos estratégicos, todo este proceso se lo ha llevado a cabo a través de las planificaciones operativas anuales de cada área, pero la decisión final para viabilizar los proyectos la mantiene la alta gerencia.

Un inadecuado tratamiento de la prioridad para la ejecución de proyectos puede ocasionar inconvenientes económicos, problemas con la disponibilidad de los servicios, incumplimientos de normativa legal e incluso pérdida de información importante para la organización.

RECOMENDACIÓN 8

El análisis de priorización y decisión de inversión para la ejecución de los proyectos debe responder a un procedimiento técnico determinado a través de la alta gerencia.

RECOMENDACIÓN 9

Aplicar una metodología de Gerencia de Proyectos para la definición y priorización de los proyectos de TI, con los componentes de evaluación del riesgo, el cumplimiento y beneficios sobre los objetivos estratégicos de la organización y el retorno de la inversión.

APO07 Gestionar los recursos humanos.

- **La gestión del talento humano no responde a una evaluación de la capacidad operativa del personal.**

El personal del área tecnológica cumple funciones ajenas a las definidas para su área con el fin de responder a requerimientos del negocio y regulaciones de organismos de supervisión y control, lo que trae consigo una sobrecarga de tareas a cubrir que no san sido planificadas.

No se han identificado planes de respaldo al personal que desarrolle y desconcentre los conocimientos en varias personas para el manejo de los procesos críticos de TI.

La externalización de la operación de servicios para ser cubierta por proveedores no se apega a políticas de confidencialidad, ni procedimientos para salvaguardar la integridad de la información que pudiera ser administrada por ellos

De acuerdo a lo que establece el marco de referencia COBIT 5, para la práctica de gestión APO07.01, dentro de la organización se debe: “Evaluar las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos empresariales. El personal incluye recursos tanto internos como externos.”

De la misma manera para la práctica de gestión APO07.01, de acuerdo al marco de referencia es necesario: “Identificar el personal clave de TI a la vez que se reduce al mínimo la dependencia de una sola persona en la realización de una función crítica

de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión y el respaldo (backup) del personal."

Para la práctica de gestión APO07.06, COBIT 5, menciona que dentro de la organización de debe: "Asegurar de que los consultores y el personal contratado que apoyan a la empresa con capacidades de TI conocen y cumplen las políticas de la organización así como los requisitos contractuales previamente acordados."

La sobrecarga de funciones y responsabilidades obedece al encargo de actividades ajenas al área de tecnología o que corresponden a requerimientos no planificados para cubrir actividades solicitadas por temas de supervisión y control, así como también al crecimiento en la entrega de servicios de tecnología como Soporte a usuarios finales, mantenimiento de aplicativos, gestión de la seguridad lógica, gestión de la infraestructura física, administración de la red local, metropolitana e internet, entre otros.

El tener una debilidad identificada con el personal asignado para el área de TI, desencadena en que el conocimiento en temas específicos esté concentrado en determinadas personas, pues no es posible en la mayoría de casos el compartir las habilidades por temas de tiempo y limitación de personal.

La cultura de redacción de documentos como políticas y procedimientos para normar la ejecución de tareas es débil dentro de la organización, lo que no ha permitido que se identifiquen responsabilidades de terceros en la ejecución de tareas contratadas.

La limitación de personal dentro del área, puede ocasionar desatención en el cumplimiento de tareas de alta prioridad con afectación en la entrega de servicios de TI críticos para el funcionamiento del negocio. De igual manera puede causar malestar e inconformidad y esto a su vez desembocar en rotación del personal dentro del área.

La concentración del conocimiento en determinadas personas puede ser contraproducente para la operación de los servicios de TI, ya que en caso de ausencia provisional o definitiva del personal, la organización se enfrentaría a retrasos o incluso paralizaciones forzadas de los servicios y esto verse reflejado en temas de pérdidas económicas y de reputación.

El no contar con reglas claras que puedan ser conocidas, compartidas y supervisadas da paso a interpretaciones de cada una de las partes en este caso con Proveedores y/o consultores, abriendo además brechas de seguridad con impacto directo en la gestión del negocio.

RECOMENDACIÓN 10

Realizar evaluaciones periódicas (auditorías de trabajo) a la gestión del personal para identificar debilidades y fortalezas dentro del área, sobrecarga de funciones y necesidades en contratación de personal para atender las exigencias propias del crecimiento del negocio y el cumplimiento de las disposiciones legales, de acuerdo a roles específicos.

RECOMENDACIÓN 11

Identificar funciones y personal clave que requieran entrenamiento cruzado para tener respaldos en caso de ausencias, y/o subrogación de funciones..

Definir el manual de funciones para el área de TI, de acuerdo a la estructura organizacional que responda al alineamiento de la organización con sus objetivos estratégicos.

RECOMENDACIÓN 11

Levantar y formalizar la documentación de los procesos y administración de servicios bajo la responsabilidad del área de TI.

RECOMENDACIÓN 12

Definir políticas y procedimientos, así como la definición de los servicios que pudieran ser atendidos a través de consultorías o entes externos.

APO08 Gestionar las relaciones.

- **La coordinación de las actividades entre áreas de la organización presenta debilidades en el enfoque de logros de objetivos comunes.**

Las áreas de negocio realizan planteamiento de solicitudes y requerimientos hacia el área de TI, sin la coordinación y evaluación de la capacidad de la atención por parte de personal e incluso obviando el escalado jerárquico para la resolución de inconvenientes que pudieran ser resueltos en su misma área.

De acuerdo al marco de referencia COBIT5, dentro de la práctica de gestión APO08.04 se deben ejecutar acciones que permitan "Trabajar con las partes interesadas y coordinar de extremo a extremo la entrega de los servicios TI y las soluciones proporcionadas al negocio."

El planteamiento de objetivos individuales para cada una de las áreas, sin visión de gestión integral para apoyar al logro de las metas que debería ser planificada y coordinada por la alta gerencia.

La falta de coordinación para la ejecución de actividades entre las áreas puede causar resquebrajamiento de las relaciones dentro de la organización y esto a su vez retrasos en la consecución de objetivos.

RECOMENDACIÓN 13

Documentar los compromisos definidos dentro de las áreas de la organización donde se identifiquen las responsabilidades sobre los procesos y objetivos del negocio y se detallen los responsables para la coordinación de actividades y el escalado jerárquico de las novedades.

APO09 Gestionar los acuerdos de servicio.

- **Los niveles en la entrega de servicios tanto internos como externos carecen de una definición para su medida y control.**.

No se ha definido un catálogo de servicios de TI que aportan a la consecución de los objetivos de la organización, y tampoco el nivel de servicio esperado por el negocio.

No existe evidencia de levantamiento y definición de niveles de servicio para clientes internos.

La supervisión y cumplimiento se realiza en función de los parámetros definidos en los contratos con los proveedores, pero al momento no se ha llegado a definir acuerdos de niveles de servicio.

Existen registros de bitácoras pero no se ha complementado con un proceso para el seguimiento de irregularidades en la entrega del servicio por parte de los proveedores.

COBIT 5 para la práctica de gestión APO09.01 sugiere:" Analizar los requisitos del negocio y el modo en que los servicios TI y los niveles de servicio soportan los procesos de negocio. Discutir y acordar servicios potenciales y niveles de servicio con el negocio y compararlos con la cartera actual para identificar servicios nuevos o modificados, u opciones de nivel de servicio."

De la misma manera para la práctica de gestión APO09.02 se espera "Definir y mantener uno o más catálogos de servicios para grupos de clientes objetivo relevantes. Publicar y mantener los servicios TI activos en los catálogos".

De acuerdo a la práctica de gestión APO09.03 se espera "Definir y preparar los acuerdos de servicio basándose en las opciones de los catálogos de servicio. Incluir acuerdos de nivel de operaciones interno".

En la práctica de gestión APO09.04 el alcance se define en “Supervisar los niveles de servicio, informar de las mejoras e identificar tendencias. Proporcionar información de gestión adecuada para ayudar a la gestión del rendimiento”

El crecimiento y diversificación de los servicios que representan el core del negocio, no ha tenido el mismo ritmo en las área que podrían considerarse estratégicas para el logro de objetivos, como el área tecnológica, en materia de inversión, innovación, capacitación del personal, interrelación con las áreas de negocio, negociación de la necesidades, evaluación de capacidades y proyecciones futuras.

La falta de definiciones en acuerdos de niveles de servicio internos puede ocasionar inconvenientes dentro de la organización ya que las áreas involucradas o usuarias de los servicios no están al tanto de las prioridades que el área de Ti brinda en la atención de un requerimiento.

Un inadecuado manejo de las relaciones con los proveedores pueden ocasionarle a la organización inconvenientes con la entrega del servicio y esto a su vez evaluado con desde el punto de vista tiempo/costo representaría pérdidas económicas para la organización.

RECOMENDACIÓN 14

Definir un catálogo de servicios dentro de la organización junto con sus responsables y su vinculación a cada uno de los procesos del negocio, incorporando el grado de criticidad e impacto para el negocio ante una contingencia.

RECOMENDACIÓN 15

Definir, negociar y formalizar acuerdos de nivel de servicio con clientes internos de acuerdo a la criticidad de los servicios definidos en el catálogo de servicios.

RECOMENDACIÓN 16

Definir, negociar y formalizar acuerdos de nivel de servicio con proveedores de acuerdo a la criticidad de los servicios definidos en el catálogo de servicios.

RECOMENDACIÓN 17

Registrar bitácoras de eventos que representen impacto a la entrega del servicio, ya sea por degradación (entrega deficiente del servicio) o interrupción total.

RECOMENDACIÓN 18

Redactar informes periódicos que resuman el comportamiento de la entrega de servicios tanto a clientes internos, como los entregados por clientes externos.

APO12 Gestionar el riesgo.

- **Dentro de la organización no se realiza una adecuada gestión de los riesgos que involucran a los servicios de TI puestos a disposición del negocio.**

El registro de información de eventos que afectan la operación y entrega del servicio de TI, se lo realiza para determinados casos.

Dentro de la organización existen evidencias de un análisis de riesgos de tecnología, pero no existe una evaluación integral del riesgo con sus componentes de probabilidad de ocurrencia y su grado de impacto al negocio, así como tampoco se

ha logrado identificar un plan de mitigación para responder ante la materialización de los riesgos.

De acuerdo a lo especificado en el marco de referencia COBIT 5, a través de la práctica de gestión APO12.01, la organización debe "Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI."

Conforme a la práctica de gestión APO12.03 es necesario "Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados."

La práctica de gestión APO12.04 menciona que la organización debe "Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada."

Las prácticas de gestión APO12.05 y APO12.06 detallan que es necesario "Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio." y "Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.", respectivamente.

La limitación del presupuesto restringe dentro de la organización la planificación de estrategias para la mitigación de los riesgos asociados a la entrega de servicios de TI.

El negocio le ha restado importancia al grado de exposición que tiene la organización ante los riesgos que ya han sido identificados y que son dados por la naturaleza de la operación y entrega de los servicios de TI.

Un inadecuado manejo de los riesgos dentro de la organización, puede traer consigo pérdidas incalculables que llegar incluso al nivel de la indisponibilidad total de la operación del servicio por periodos indeterminados.

RECOMENDACIÓN 19

Realizar una evaluación integral y análisis de riesgos de los servicios de tecnología con sus componentes de probabilidad de ocurrencia y su grado de impacto al negocio.

RECOMENDACIÓN 20

Establecer estrategias para la mitigación de los riesgos dentro de la organización de acuerdo a su grado de exposición.

RECOMENDACIÓN 21

Calendarizar y ejecutar las estrategias de mitigación de riesgos con mayor grado de exposición e impacto para el negocio.

RECOMENDACIÓN 22

Definir y verificar periódicamente planes de respuesta para minimizar el impacto cuando ocurren incidentes de riesgo.

APO13 Gestionar la seguridad.

- **La seguridad de la información lógica y física se muestra como un eslabón débil dentro de la organización.**

Se han determinado acciones básicas de control principalmente orientadas a la gestión de la seguridad física y acceso al cuarto de servidores y equipos de telecomunicaciones, que no cubren un nivel de gestión deseable para la organización.

La seguridad lógica no tiene un tratamiento integral, sino más bien se lo maneja de forma aislada para atacar la exposición a vulnerabilidades comunes como virus, spam o spyware.

Para la práctica de gestión APO13.01 se debería, "Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa."

De igual manera la práctica de gestión APO13.02, es necesario," Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio."

Respecto a la práctica de gestión APO13.03, busca" Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de

información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua."

La principal causa para el débil tratamiento de la gestión de seguridad es la ausencia de una normativa interna que determine los controles a aplicar y sobre los cuales se debería realizar evaluaciones.

El no tomar acciones efectivas para equiparar la necesidad de controles en seguridad de la información, puede traer consigo la materialización de riesgos y esto a su vez efectos negativos a nivel económico, reputacionales e incluso poner en riesgo al negocio como tal.

RECOMENDACIÓN 23

Definir políticas de seguridad de la información tanto física como lógica que abarque el tratamiento de los riesgos relacionados.

RECOMENDACIÓN 24

Establecer un plan de tratamiento de los principales riesgos de la seguridad de la información, de acuerdo a las mejores prácticas establecidas en los marcos de referencia como las Normas de Seguridad de la Información ISO- 27001, ISO 27002.

RECOMENDACIÓN 25

Realizar un seguimiento periódico del cumplimiento de las políticas de seguridad de la información y la aplicación del plan de tratamiento de los riesgos.

BAI08 Gestionar el conocimiento

- **La documentación para gestionar el conocimiento está enfocada en los procesos principales y no se alimenta una base general para la resolución de inconvenientes.**

El personal del área de TI tiene como prioridad la atención de actividades operativas planificadas y la documentación no está inmersa dentro de esta definición.

Los datos se registran pero no tienen un mantenimiento continuo, por lo que la información disponible está desactualizada o incompleta.

Es tarea de la Gestión del Conocimiento, en primera instancia, transmitir a todos los miembros de la organización TI la importancia de registrar la información relacionada con su trabajo en las herramientas dispuestas para ello.

Por otro lado, es también su labor instalar una cultura de aprendizaje constante entre los miembros del personal. No sólo se trata de hacer que los empleados registren los datos, sino también motivarlos a que acudan a las fuentes de conocimiento para completar aquello que no saben.

La Gestión del Conocimiento debe garantizar que la información disponible sea completa y esté puntualmente actualizada, ya que de otro modo puede resultar inútil.

El propósito primordial de esta gestión es mejorar la eficiencia reduciendo la necesidad de redescubrir conocimientos.

Un manejo inadecuado del conocimiento puede ocasionar dentro de la organización retrasos en la solución de inconvenientes al buscar soluciones para temas que en algún momento ya fueron identificadas.

RECOMENDACIÓN 26

Definir una estrategia de gestión del conocimiento que permitan mantener en una fuente confiable de información el aprendizaje diario dentro de la organización y que esta aporte a la toma de decisiones importantes.

RECOMENDACIÓN 27

Determinar las fuentes principales de conocimiento dentro de la organización, con el fin de establecer los planes necesarios para su transferencia, su disponibilidad y aporte para el cumplimiento de los objetivos.

DSS01 Gestionar operaciones

- **La administración de operaciones se la maneja como una función operativa dentro de las tareas del día a día.**

Dentro de la organización no se cuenta con procedimiento formalizado de monitoreo de la operación de los servicios de tecnología.

Los servicios de tecnología no se hallan categorizados de acuerdo a su criticidad para la operación del negocio.

Se identificaron escasas medidas de protección para garantizar el entorno de las instalaciones de TI.

La gestión de las instalaciones como por ejemplo las fuentes de energía, sistemas de enfriamiento, la gestión del acceso a dependencias, el monitoreo de ambientes, cableado estructurado, etc. no se han manejado a través de procedimientos técnicos que incluyan aplicación de mejores prácticas, estándares y regulaciones.

De acuerdo al marco de referencia COBIT 5, a través de la práctica de gestión DSS01.01 se debe "Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente".

Así mismo, en la práctica de gestión DSS01.02 menciona que es necesario "Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio".

Para la práctica de gestión DSS01.03 se busca "Supervisar la infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones"

.De forma similar a través de la práctica de gestión DSS01.04 es necesario "Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno".

Por última la práctica de gestión DSS01.05, Establece la necesidad de "Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo".

RECOMENDACIÓN 28

Definir procedimientos estandarizados que permitan monitorear la disponibilidad de los servicios a través del correcto funcionamiento de los componentes que intervienen durante todo el proceso hasta la entrega.

RECOMENDACIÓN 29

Realizar una revisión integral para identificar deficiencias en las instalaciones físicas respecto a las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.

RECOMENDACIÓN 30

Ejecutar acciones correctivas que permitan remediar las deficiencias identificadas y garantizar una adecuada gestión de las instalaciones físicas, disminuyendo el riesgo en la operación de los servicios.

DSS03 Gestionar problemas.

- **Los problemas relacionados con los servicios de TI, no responden a un proceso definido para su atención y en la mayoría de casos se los maneja con informalidad.**

La identificación y clasificación de problemas no forma parte del trabajo planificado como tareas de gestión dentro del área de TI.

No se ha considerado la ejecución de estrategias para el tratamiento de problemas a través de un registro, priorización y conocimiento del estado de avance en la solución.

Al no existir una clasificación explicita de los problemas, la gestión proactiva es una tarea pendiente para la organización

El marco de referencia COBIT 5, a través de la práctica de gestión DSS03.01 menciona que se debe "Definir e implementar criterios y procedimientos para informar de los problemas identificados, incluyendo clasificación, categorización y priorización de problemas."

De la misma forma a través de la práctica de gestión DSS03.02, define que en la organización es importante "Investigar y diagnosticar problemas utilizando expertos en las materias relevantes para valorar y analizar las causas raíz."

Para el levantamiento de errores conocidos se busca con la práctica de gestión DSS03.03 "Tan pronto como las causas raíz de los problemas se hayan identificado, crear registros de errores conocidos y una solución temporal apropiada, e identificar soluciones potenciales."

A través de la práctica de gestión DSS03.04, se menciona “Identificar e iniciar soluciones sostenibles refiriéndose a la causa raíz, levantando peticiones de cambio a través del proceso de gestión de cambios establecido si se requiere para resolver errores. Asegurarse de que el personal afectado está al tanto de las acciones tomadas y de los planes desarrollados para prevenir que vuelvan a ocurrir futuros incidentes.”

Finalmente, la práctica de gestión DSS03.05 recomienda “Recoger y analizar datos operacionales (especialmente registros de incidentes y cambios) para identificar tendencias emergentes que puedan indicar problemas. Registrar problemas para permitir la valoración.”

El negocio no se interesa en evaluar procedimientos complementarios que pueden elevar el nivel en la entrega del servicio.

El personal del área de Ti no se halla familiarizado con marcos de referencia que proponen prácticas comprobadas para la atención y gestión de problemas.

La falta de un diagnóstico integral de gestión de riesgos dificulta le ejecución de planes de tratamiento de problemas proactivos.

Un inadecuado tratamiento de los problemas puede generar entre otras cosas pérdidas económicas para el negocio, perdidas de información, esfuerzo y trabajo repetitivo para atender incidentes similares, retrasos o incumplimientos de normativas legales.

RECOMENDACIÓN 31

Definir un procedimiento general para la atención de problemas identificando prioridad, criticidad y urgencia en los servicios así como los responsables para la atención y seguimiento hasta la solución.

RECOMENDACIÓN 32

Generar registros de la soluciones brindadas a errores conocidos para alimentar la base de conocimiento general para la entrega de los servicios de TI.

RECOMENDACIÓN 33

Coordinar con las áreas de negocio reuniones periódicas para evaluar la importancia del tratamiento de problemas y su compromiso frente a las estrategias propuestas por el área de TI.

7. Observaciones de la aplicación del modelo

- **Existen procedimientos de tecnología demasiado rigurosos aún para alcanzar un nivel de capacidad 1.**

La organización no se hallaba preparada para una evaluación con los niveles de exigencia definidos en el modelo aplicado.

La SEPS busca definir y aplicar medidas uniformes para conocer el estado real de la capacidad de los procesos de TI dentro de las organizaciones supervisadas.

La organización no ha sido sometida a procedimientos de evaluación externos así como tampoco se han realizado procedimientos de autoevaluación para conocer la situación de sus procesos.

RECOMENDACIÓN 1

Para los casos en los que el impacto en la gestión del procedimiento demanda de esfuerzo e inversión considerables, se deberían acordar en conjunto las estrategias que provoquen un menor impacto para encaminarlas hacia el nivel de capacidad determinado.

- **Los niveles de capacidad utilizados para la evaluación de los procesos no resultan familiares para los entrevistados.**

La organización no ha participado de procedimientos de evaluación para conocer el grado de madurez de sus procesos, incluso a nivel general.

La SEPS busca definir y aplicar medidas uniformes para conocer el estado real de la capacidad de los procesos de TI dentro de las organizaciones supervisadas, a través de la aplicación de un lenguaje común como los criterios de evaluación y los niveles de capacidad.

La evaluación de la capacidad de los procesos, así como procedimientos generales de evaluación de cumplimiento son temas relativamente nuevos que vienen de la mano con las regulaciones y supervisión que empieza a ejercer la SEPS como ente de control, y han sido manejados de forma aislada sin conocer y aplicar prácticas o marcos de referencia ampliamente conocidos.

RECOMENDACIÓN 2

Previa la aplicación del modelo, es necesario desplegar un programa de capacitación y entrenamiento al personal de las organizaciones reguladas acerca de las generalidades del Modelo a aplicar, así como sus objetivos, ventajas y beneficios para las organizaciones.

8. Conclusiones de la evaluación para la organización

- La organización de acuerdo al análisis de capacidad de sus procesos se encuentra en un NIVEL 1, lo que muestra que se halla encaminada al cumplimiento de los objetivos planteados, a pesar de que aún no entrega los resultados esperados para todos los procesos evaluados.

- Utilizando la definición para la determinación del nivel de madurez, las organizaciones cuya capacidad de procesos se encuentren en Nivel 1, se corresponderán con un Nivel de Madurez 1, teniendo como tareas pendientes la atención de las recomendaciones formuladas después del análisis realizado.

9. Conclusiones de la aplicación del modelo

- La organización que participó en la prueba piloto del modelo, brindó las facilidades para la evaluación, ya que estaba interesada en conocer la

capacidad de sus procesos de TI y las mejoras que podrían aplicarse para impulsar el mejoramiento integral.

- La aplicación de la prueba piloto del modelo construido, generó los resultados esperados ya que mediante la utilización de las plantillas preparadas para la calificación de los niveles de capacidad, se logró determinar el nivel de madurez para la organización de acuerdo a los parámetros definidos.

- A través de la aplicación de la prueba piloto se verificó que los procesos definidos dentro del modelo guardan relación con los procesos tecnológicos gestionados dentro de la organización ya sea de manera formal o informal.

CAPITULO V

5.1 Conclusiones y Recomendaciones

5.1.1 Conclusiones

- El desarrollo del modelo se realizó mediante un análisis de los principales procesos tecnológicos de las organizaciones supervisadas por la SEPS, y a través de un procedimiento de priorización se definieron 22 procesos con mayor impacto sobre el propósito fundamental de supervisión y control.
- La base para el desarrollo del modelo de Madurez Tecnológico, fue el marco de referencia COBIT, junto con su modelo de evaluación de capacidad de procesos basado en la norma ISO/IEC 15504, además del aporte del Marco de Gestión de Servicios ITIL V3 2011 y la norma de seguridad de la información ISO 27001, utilizados como criterios de evaluación.
- Para la evaluación de capacidad de los procesos tecnológicos se definieron plantillas que permiten recoger los criterios de cumplimiento de las actividades por cada una de las prácticas de gestión tanto para el Nivel 1 como para los Niveles del 2 a 5, generando los resultados a partir de los criterios de calificación.
- A través del análisis de los resultados de la prueba piloto se pudieron generar recomendaciones para el mejoramiento de los procesos y la gestión integral de la organización, así como también determinar el nivel de Madurez en el que esta encuentra, respecto al criterio definido dentro del modelo de madurez.

- El modelo propuesto a través de la aplicación de la prueba piloto generó los resultados esperados, por lo tanto, se puede confirmar su aplicabilidad y robustez para la evaluación del nivel de madurez en las organizaciones supervisadas por la SEPS.
- Los resultados obtenidos de la evaluación y prueba del modelo de madurez pueden servir como base para el análisis de la generación de un marco normativo que les permita a las organizaciones supervisadas conocer e implementar estrategias comunes que contribuyan a la gestión de los riesgos a partir de su componente tecnológico.
- El Modelo propuesto apoyará de manera sustancial a la construcción y fortalecimiento del proceso metodológico de supervisión llevado a cabo por parte de parte de la SEPS, a través de la estandarización de procesos y la homologación de criterios para su evaluación.

5.1.2 Recomendaciones

- La priorización de los procesos incluidos en el modelo desarrollado responde a la situación definida en el momento del análisis, sin embargo deberían evaluarse de acuerdo a la evolución, nuevos requerimientos y propuestas determinados por la SEPS para con las organizaciones supervisadas.
- Difundir la implementación de marcos de referencia mundialmente aceptados como los utilizados en el desarrollo de la presente propuesta, para la gestión de los procesos de TI dentro de las organizaciones supervisadas.

- Las plantillas elaboradas responden a las especificaciones del Modelo, por lo que el uso de esta herramienta es obligatorio para la valoración de los procesos.
- Evaluar la capacidad de las organizaciones para implementar las novedades identificadas, así como los plazos para su remediación y cumplimiento.
- Utilizar el presente modelo como una herramienta de apoyo y mejora a los procesos de supervisión y control.
- La SEPS debería generar el marco normativo base para la gestión de las tecnologías de la información como componente de la gestión del riesgo dentro de las organizaciones supervisadas, que permita darle un mayor peso al proceso de evaluación de capacidad de sus procesos.

BIBLIOGRAFÍA

Ortega de la Torre, A. (s.f.). *Cobit 4.* Obtenido de http://ds5-andre-ortega-5a.host56.com/historia.html

RIVERA GUZMAN, S., & ALVAREZ GUAPACHA, C. E. (2012). Obtenido de http://bibliotecadigital.icesi.edu.co/biblioteca_digital/bitstream/10906/68026/1/modelo_madurez_educacion.pdf

Superintendencia de Bancos y Seguros. (26 de 04 de 2012). *Superintendencia de Bancos y Seguros.* Obtenido de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf

Villegas, M., Viloria, O., & Blanco, W. (s.f.). Obtenido de http://www.laccei.org/LACCEI2009-Venezuela/p188.pdf

Acevedo Juárez, H. (11 de 08 de 2011). *Magazcitum*. Recuperado el 27 de 07 de 2013, de http://www.magazcitum.com.mx/?p=1574

Cano, C., Fernández Sanz, L., Pages, C., Villalba, M., Temesio, S., & Motz, R. (2012). *www.esvial.org.* Obtenido de http://www.esvial.org/wp-content/files/Atica2012_pp101-109.pdf

Cedeno, M. (2012). *La Transicion de COBIT 4.1 a COBIT 5.*

Crisoltic. (8 de 4 de 2012). *Crisoltic*. Obtenido de http://www.crisoltic.com/2012/04/cobit-5-que-hay-de-nuevo.html

Diez, M. (06 de 2004). *Capability Maturity Model Integration.* Recuperado el 2013 de 07 de 27, de http://www.ing.unp.edu.ar/asignaturas/is/papers/CMMI%20i.pdf

Ediciones Legales Informacion Adicional. (s.f.). *Ediciones Legales Informacion Adicional.* Obtenido de http://www.edicioneslegales-informacionadicional.com/leyes/LeysistemaFinancieroultima.pdf

Garzas, J., Fernandez, C., & Piattini, M. (09 de 2009). *http://www.ati.es/*. Obtenido de http://www.ati.es/IMG/pdf/GarzasVol5Num2.pdf

http://prezi.com/7saajphdnw7c/copy-of-cobit-5/. (s.f.).

INGERTEC. (s.f.). *INGERTEC*. Obtenido de http://ingertec.com/iso-15504

IS&BCA. (s.f.). *Information Segurity& Business Continuity Academy*. Recuperado el 27 de 07 de 2013, de http://www.iso27001standard.com/es/que-es-la-norma-iso-27001

Isaca - Cobit 5. (1013). *Process Assessment Model Cobit 5*.

ISACA. (2012). Procesos Catalizadores. Estados Unidos.

Isaca. (s.f.). *COBIT 5 Introducción - Presentación de PowerPoint - isaca*. Obtenido de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CDkQFjAC&url=http%3A%2F%2Fwww.isaca.org%2FCOBIT%2FDocuments%2FCOBIT5-Introduction-Spanish.ppt&ei=c-gCUsr8LYP88gSiuYHYDA&usg=AFQjCNHwaWjs0bKzkjEJ4dgoNAs1BrCKvA&bvm=bv.50310824,d.eWU&ca

ISACA.ORG. (s.f.). *ISACA.ORG*. Obtenido de http://www.isaca.org/COBIT/Documents/COBIT5-Framework-Spanish.pdf

ISO27000. (s.f.). *ISO27000.ES*. Obtenido de http://www.iso27000.es/iso27000.html#section3c

IT_GRC, Franco. (s.f.). *IT – Governance, Risk & Compliance*. Obtenido de http://francoitgrc.wordpress.com/2012/04/14/cobit-5-update-por-version-oficial-de-isaca/

IT_GRC, Franco;. (s.f.). *IT – Governance, Risk & Compliance*. Obtenido de http://francoitgrc.wordpress.com/2012/04/14/cobit-5-update-por-version-oficial-de-isaca/

ITIL. (s.f.). *ITIL*. Obtenido de http://www.itil-officialsite.com/

Junta de Regulacion del SFPS. (29 de 10 de 2012). *SEPS*. Recuperado el 2013, de http://www.seps.gob.ec/c/document_library/get_file?uuid=7352a858-e24d-4269-b747-03ce40cb89b8&groupId=10157

Machado, N., & Ramirez, S. (2012). Obtenido de http://www.ccee.edu.uy/jacad/2012/x%20area%20y%20mesa/CONTABILIDAD-ADMINISTRACION/1-contabilidad%20de%20gestion/3-Analisis%20del%20estado%20de%20madurez%20de%20la%20gestion%20de%20riesgo%20en%20el%20sector%20servicios%20del%20Uruguay.pdf

Palomino Vasquez, M. A. (11 de 2011). *Repositorio General de Tesis PUCP*. Obtenido de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1524/PALOMINO_VASQUEZ_MARCO_COMPETOSOFT_LIM_LAMBDA.pdf?sequence=1

Pino, F., Garcia, F., Ruiz, F., & Piattini, M. (4 de 2006). *IEEE Advancing Technology for Humanity*. Obtenido de http://www.ewh.ieee.org/reg/9/etrans/ieee/issues/vol04/vol4issue2April2006/4TLA2_04Pino.pdf

Pino, F., Serrano, M., García, F., Piattini, M., & Oktaba, H. (12 de 2006). *Competisof*. Obtenido de http://alarcos.inf-cr.uclm.es/competisoft/publico/downloads/Inf_T%C3%A9cnicos/COMPETISOFT_IT_3.pdf

Ramirez, F. (09 de 05 de 2012). *Blog SPICE/ISO /IEC 15504*. Obtenido de http://seispice.blogspot.com/2012/05/spiceiso-iec-15504-norma-spiceiso-iec.html

REPÚBLICA DEL ECUADOR- SUPERINTENDENCIA DE BANCOS Y SEGUROS. (s.f.). *REPÚBLICA DEL ECUADOR- SUPERINTENDENCIA DE BANCOS Y SEGUROS*. Recuperado el 27 de 07 de 2013, de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_V.pdf

Rivera G., S. P., & Alvarez G, C. E. (2012). Obtenido de http://bibliotecadigital.icesi.edu.co/biblioteca_digital/bitstream/10906/68026/1/modelo_madurez_educacion.pdf

RSFPS. (29 de 10 de 2012). *Superintencia de Economia Popular y Solidaria.* Obtenido de http://www.seps.gob.ec/c/document_library/get_file?uuid=7352a858-e24d-4269-b747-03ce40cb89b8&groupId=10157

Saffirio, M. (21 de 06 de 2008). *http://msaffirio.wordpress.com/*. Recuperado el 27 de 07 de 2013, de http://msaffirio.wordpress.com/2008/06/21/escala-de-madurez-%E2%80%93-process-maturity-model/

SEPS. (05 de 04 de 2011). *SEPS- LEY ORGANICA DE LA ECONOMIA POPULAR Y SOLIDARIA Y DEL SECTOR* . Recuperado el 2013, de http://www.seps.gob.ec/c/document_library/get_file?uuid=4d879bbc-2bbc-47db-a27d-09642ef8a0c7&groupId=10157

SEPS. (16 de 02 de 2012). *SEPS.* Recuperado el 2013, de http://www.seps.gob.ec/c/document_library/get_file?uuid=dda0d545-4998-4b61-9bd9-7185090766ef&groupId=10157

Sperat, S. O. (s.f.). *Estratega*. Recuperado el 26 de 07 de 2013, de http://estratega.org/site/todo-lo-que-usted-queria-saber-sobre-cobit-5-y-no-se-animo-a-preguntar/

Superintendencia de Bancos y Seguros. (s.f.). *Republica del Ecuador-Superintendencia de Bancos y Seguros.* Recuperado el 27 de 07 de 2013, de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_V.pdf

Taylor, S., & Turbitt, K. (s.f.). *bmcsoftware.* Obtenido de http://documents.bmc.com/products/documents/74/14/87414/87414.pdf

ANEXOS

ANEXO 1

ANEXO 2

ANEXO 3